

# Logic of Intuitionistic Interactive Proofs (Formal Theory of Perfect Knowledge Transfer)\*

Simon Kramer

`simon.kramer@a3.epfl.ch`

November 7, 2018

## Abstract

We produce a decidable *super-intuitionistic* normal modal logic of internalised *intuitionistic* (and thus disjunctive and monotonic) interactive proofs (LiP) from an existing classical counterpart of classical monotonic non-disjunctive interactive proofs (LiP). Intuitionistic interactive proofs effect a durable epistemic impact in the possibly adversarial communication medium CM (which is imagined as a distinguished agent) *and only in that*, that consists in the permanent induction of the *perfect* and thus *disjunctive* knowledge of their proof goal by means of CM’s knowledge of the proof: If CM knew my proof then CM would persistently and also *disjunctively* know that my proof goal is true. So intuitionistic interactive proofs effect a lasting transfer of disjunctive propositional knowledge (disjunctively knowable facts) in the communication medium of multi-agent distributed systems via the transmission of certain individual knowledge (knowable intuitionistic proofs). Our (necessarily) CM-centred notion of proof is also a disjunctive explicit refinement of KD45-belief, and yields also such a refinement of standard S5-knowledge. Monotonicity but not communality is a commonality of LiP, LiP, and their internalised notions of proof. As a side-effect, we offer a short internalised proof of the Disjunction Property of Intuitionistic Logic (originally proved by Gödel).

**Keywords:** agents as proof-checkers; communication networks; constructive Kripke-semantics; disjunctive explicit doxastic & epistemic logic; interactive & oracle computation; interpreted communication; intuitionistic modal logic; multi-agent distributed systems; proofs as sufficient evidence.

## 1 Introduction

**Subject matter** The subject matter of this paper is normal modal logic of internalised monotonic interactive proofs, i.e., a novel super-intuitionistic nor-

---

\*Work partially funded with Grant AFR 894328 from the National Research Fund Luxembourg cofunded under the Marie-Curie Actions of the European Commission (FP7-COFUND) [Kra13a].

mal modal logic of internalised intuitionistic (and thus disjunctive and monotonic) interactive proofs (LliP) as well as an existing classical normal modal logic of internalised classical monotonic (and thus non-disjunctive) interactive proofs (LiP) [Kra12a, Kra13c]. (We abbreviate interactivity-related adjectives with lower-case letters.) Recall from [Mos10] that a super-intuitionistic propositional logic is any consistent collection of propositional formulas that contains all the axioms of Intuitionistic Propositional Logic (IL) and that is closed under *modus ponens* and substitution of arbitrary formulas for proposition letters. Note however that the *language* of IL is a strict subset of the (propositionally modal) language of LliP.

**Goal** Our goal here is to produce LliP axiomatically as well as semantically from LiP. The process of constructing LliP from LiP is presented for the sake of gaining insight into the semantic connection between intuitionistic and classical interactive proofs, respectively. LliP, the result of the construction, however is independent of LiP. Further note that like in [Kra12a], [Kra12c, Kra13c], and [Kra12b, Kra13b], we still understand interactive proofs as *sufficient evidence* for intended resource-unbounded proof-checking agents (who are though unable to guess), and leave probabilistic and polynomial-time resource bounded agents for future work. Finally note that we choose our meta-logic to be classical (singleton meta-universe or meta-world unicity, cf. Section 1.1.1).

## 1.1 Motivation

Our immediate motivation for LliP is to complete the picture of our above-mentioned resource-unbounded propositional normal modal logics of interactive proofs with the missing variant of intuitionistic interactive proofs—see Table 1. The overarching motivation for LliP is to serve in an intuitionistic foundation of interactive computation. See [Kra12a] for a programmatic motivation. Table 1 displays characteristic properties of our interactive proofs as internalised in their respective resource-unbounded propositional normal modal logic together with typical applications in information security. The logics themselves, in contrast to their internalised proof terms, except LliP are classical, i.e., monotonic and non-disjunctive (and thus negation-incomplete). As a confirmation, notice that disjunctivity is a necessary but not sufficient condition for intuitionism.

We recall and explain all this logical terminology in the next subsections, and thereby draw some inspiration from the quite different intuitionistic logic of intuitionistic non-interactive proofs [AI07] and from the informational views on modal and intuitionistic logic expressed in [vB97, vB09].

### 1.1.1 Intuitionistic Logic (IL)

**Definition** From [Mos10], recall that Intuitionistic Propositional Logic (IL) can be succinctly described as Classical Propositional Logic without the Aristotelian law of excluded middle (LEM):  $(A \vee \neg A)$ , but with the law of contradiction  $(\neg A \rightarrow (A \rightarrow B))$ , and that intuitionistically, *Reductio ad absurdum*

Table 1: Proof-term properties

	classicality	communality	disjunctivity (constructivity)	monotonicity
<b>LiP</b> <i>intuitionistic</i>		non-communal ( <i>communication-medium</i> or <i>-adversary</i> centred [Gol11, Chapter 16])	<i>disjunctive</i> , negation- <i>incomplete</i>	monotonic
<b>LiP</b> [Kra12a, Kra13c]	classical	common knowledge (security-infrastructure or <i>meta</i> -modelling: clocks [FSK10, Chapter 16], names [And08, Chapter 6], PKIs [FSK10, Chapter 18–20])	non-disjunctive, negation- <i>incomplete</i>	monotonic
<b>LiP</b> [Kra12c, Kra13c]	classical	common belief (security <i>object</i> -models: access control [And08, Chapter 4], [Gol11, Chapter 5, 20]; data-base security [Gol11, Chapter 9]; communication protocols [And08, Chapter 3], [Gol11, Chapter 16], [FSK10, Chapter 13])	non-disjunctive, negation- <i>incomplete</i>	non-monotonic
<b>LDiP</b> [Kra12b, Kra13b]	classical	non-communal ( <i>arbitrary-single-agent</i> <i>centred</i> : <i>network</i> -adversaries [And08, Chapter 21], [Gol11, Chapter 17]; reference monitors [Gol11, Chapter 6])	<i>disjunctive</i> , <b><i>negation- complete</i></b>	non-monotonic

only proves negative statements, since  $(\neg\neg A \rightarrow A)$  does not hold in general. (If it did, LEM would follow by *modus ponens* from the intuitionistically provable  $\neg\neg(A \vee \neg A)$ .) Semantically, IL (and LIIP) is perhaps best viewed as a modal logic [Kri65] (cf. Definition 5 and Table 2). Therein,

- the valuation function on atomic propositions is constrained to be monotonic with respect to a partial order on system states (possible worlds);<sup>1</sup>
- the positive intuitionistic connectives (conjunction, disjunction) are interpreted as their classical counterparts (which conserve the monotonicity of atomic propositions) on the current state;
- the negative intuitionistic connectives (negation, implication) are interpreted as their non-monotonic classical counterparts on *the upset of the current state with respect to the partial order* (and thus *are made to* conserve the monotonicity of atomic propositions).

Hence first, intuitionistic negation and implication can be viewed as classical negation and implication prefixed by a (unary) modality that is interpreted by a (binary) partial-order accessibility relation (e.g., a temporal reachability relation), respectively; and second, intuitionistic facts, be they positive or negative, are necessarily monotonic (durable, forward invariant, lasting, persistent, stable) in the state space [vB09]. (Intuitionistic double negation can be interpreted temporally as the forward invariant “at some future time.”) Plain classical logic is also but trivially monotonic, as it can be viewed as a modal logic over a singleton state space. From this modal viewpoint, one immediately recognises why  $(\neg\neg A \rightarrow A)$  (“true at some future time implies true now”) is valid classically.

**Properties** In the previous paragraph, we saw that IL has the monotonicity property (“*intuitionistic* implies *monotonic*”). IL has also the important disjunction property (“*intuitionistic* implies *disjunctive*”). That is, any external intuitionistic notion of proof  $\vdash_I$  has the property that  $\vdash_I A \vee B$  implies  $\vdash_I A$  or  $\vdash_I B$ . Recall that disjunctivity is a necessary but not sufficient condition for intuitionism, and that plain classical notions of proof do not have the disjunction property. Now note that when internalised in an object-logical language,

- an external intuitionistic notion of proof, say  $\vdash_{I_1}$ , becomes a unary necessity modality, say  $[M]$ , parametrised with a proof term  $M$ ;
- the disjunction property of  $\vdash_{I_1}$  becomes a disjunctive property of the internalising external notion of proof, say  $\vdash_{I_2}$ , that  $\vdash_{I_2} [M](\phi \vee \phi') \rightarrow ([M]\phi \vee [M]\phi')$ ;

---

<sup>1</sup>Incidentally, this monotonicity makes intuitionistic logic incompatible with hybrid logic, whose nominals are atomic propositions true at a single state [AtC07], at least in the basic case where the intuitionistic-logical universe of worlds coincides with the hybrid-logical one. For more complex cases, see for example the work of Torben Braüner and Valeria de Paiva.

- the monotonicity property becomes the similar property that  $\vdash_{I_2} [M]\phi \rightarrow [(M, M')]\phi$ , where  $(M, M')$  is the term pair constructed from  $M$  and  $M'$  with  $M'$  representing the additional data allowed by the monotonicity.

Further note that a normal modal logic that internalises an intuitionistic notion of proof is necessarily intuitionistic itself: assume that the external notion of proof, say  $\vdash$ , is classical, i.e.,  $\vdash \phi \vee \neg\phi$ , and deduce  $\vdash [M](\phi \vee \neg\phi)$  by the normal-modal rule schema of necessitation that  $\vdash \phi$  implies  $\vdash [M]\phi$ . So the internalised notion of proof  $[M]$  is classical too. Even a non-normal modal logic like [AI07] must be intuitionistic itself in order to be able to internalise an intuitionistic notion of proof, because already [AI07]’s weaker form of necessitation—that  $\vdash_{\text{ILP}} F$  implies that *there is a* proof term  $t$  such that  $\vdash_{\text{ILP}} t : F$ —forces external intuitionism. Finally note that IL is algorithmically decidable [Sta79].

### 1.1.2 Negation-complete logics

**Definition** Recall that a notion of proof, say  $\vdash_1$ , is *negation-complete* by definition if and only if  $\vdash_1 A$  or  $\vdash_1 \neg A$ . When internalised in an object language with an external notion of proof, say  $\vdash_2$ , negation completeness becomes  $\vdash_2 [M]\phi \vee [M]\neg\phi$ . Though conveniently classical (LEM), negation-complete logics have also the property of having constructive and computational content.

**Properties** From the detailed reminder in Section 1.1.1 of [Kra12b, Kra13b], recall that first, the negation-completeness property implies the discussed disjunction property (“*negation-complete* implies *disjunctive*”); second, any internalised negation-complete notion of proof  $\vdash_2$  is non-monotonic, that is,  $\vdash_2 [M]\phi \vee [M]\neg\phi$  implies  $\not\vdash_2 [M]\phi \rightarrow [(M, M')]\phi$  (“*negation-complete* implies *non-monotonic*”); third, negation completeness and intuitionism are incompatible properties; and fourth, negation completeness implies algorithmic decidability.

### 1.1.3 Communality

In LDiiP, LiiP, LiP, and LliP, our so-far *ad hoc* modal notation  $[M]\phi$  becomes  $M \vee_a \phi$ ,  $M ::^{\mathcal{C}}_a \phi$ ,  $M :^{\mathcal{C}}_a \phi$ , and  $M \pm_{\mathbf{CM}} \phi$ , respectively, where  $a$  and  $\mathcal{C}$  is an additional parameter for a peer-reviewing agent  $a$  (such as the as-an-agent-imagined communication medium  $\mathbf{CM}$ ) and a finite agent-community  $\mathcal{C}$  of peers, respectively. The intended meaning of these modalities is “ $M$  can classically and disjunctively but only non-monotonically prove to  $a$  that  $\phi$  [is true],” “ $M$  can classically and non-monotonically prove to  $a$  that  $\phi$  and this fact is common belief in  $\mathcal{C} \cup \{a\}$ ,” “ $M$  can classically and monotonically prove to  $a$  that  $\phi$  and this fact is common knowledge in  $\mathcal{C} \cup \{a\}$ ,” and “ $M$  can intuitionistically (and thus disjunctively and monotonically) prove to  $\mathbf{CM}$  that  $\phi$ ,” respectively. (Recall from [FHMV95, MV07], that knowledge implies belief.) In all these logics, the proof potential is such that if my peer reviewer knew my proof then she would know that its proof goal is true. Notice that what is accepted as a potential proof  $M$  may depend on a community  $\mathcal{C} \cup \{a\}$  of peers if and only if the proof is non-disjunctive. This is the (non-)communality of  $M$  mentioned in Table 1.

## 1.2 Contribution

Our contribution in this paper is five-fold:

1. We produce the intuitionistic Logic of Intuitionistic interactive Proofs (LIiP) (cf. Theorem 3) from its classical counter-part LiP. LIiP internalises necessarily *communication-medium-centred* (or *communication-adversary-centred*)<sup>2</sup> intuitionistic proof theories, enjoying the disjunction property. As notable *syntactic novelties* in intuitionistic modal logic, LIiP provides:
  - (a) a non-primitive
    - i. possibility modality that is *doubly macro-definable* within the language of LIiP: in terms of double negation and
      - A. communication-medium knowledge (cf. Page 9),
      - B. its corresponding primitive necessity modality (though *not* in the classical modal terms  $\Diamond\phi \leftrightarrow \neg\Box\neg\phi$ , cf. Theorem 2.58);
    - ii. necessitation rule that is derivable from the primitive modal monotonicity axiom schema  $\phi \rightarrow \Box\phi$  and the primitive *modus ponens* deduction rule (cf. Theorem 2.0);
  - (b) the two insights that in interactive settings,
    - i. the intuitionistic truths are those of the communication medium (cf. Remark 2),
    - ii. intuitionistic proofs induce perfect and thus disjunctive knowledge in the communication medium, and only in that (cf. Remark 3).

That is, we put forward *LIiP as a modal-logical characterisation of the concept of message-passing communication medium*.

2. We provide a standard but also oracle-computational and set-theoretically constructive Kripke-semantics for LIiP (cf. Section 2.2):
  - Like in [Kra12c, Kra13c] and [Kra12b, Kra13b], we endow the proof modality with a standard Kripke-semantics [BvB07], but first define its accessibility relation  ${}_M\mathcal{R}_{\text{CM}}$  constructively in terms of elementary set-theoretic constructions,<sup>3</sup> namely as  ${}_M\mathbf{R}_{\text{CM}}$  (cf. Section 2.2.1), and then match it to an abstract semantic interface in standard form (which abstractly stipulates the characteristic properties of the accessibility relation [Fit07]). We will say that  ${}_M\mathbf{R}_{\text{CM}}$  *exemplifies* (or *realises*)  ${}_M\mathcal{R}_{\text{CM}}$  (cf. Section 2.2.2). (A simple example of a set-theoretically constructive but non-intuitionistic definition of a modal accessibility is the well-known definition of epistemic accessibility

<sup>2</sup> In communication security, the communication medium is usually assumed adversarial (as an agent) and called Eve (the eavesdropper).

<sup>3</sup> in loose analogy with the set-theoretically constructive rather than the purely axiomatic definition of numbers [Fef89] or ordered pairs (e.g., the now standard definition by Kuratowski, and other well-known definitions [Mos06])

as state indistinguishability defined in terms of equality of state-projection functions [FHMV95].)

- Our Kripke-semantics is oracle-computational in the sense that the individual proof knowledge (say  $M$ ) can be thought of as being provided by a computation oracle (cf. Definition 3), which thus acts as a hypothetical provider and imaginary epistemic source of our interactive proofs.

As notable *semantic novelties* in intuitionistic modal logic, LliP is:

- (a) *doubly constructive*: LliP is an intuitionistic (and thus constructive) logic and additionally offers a set-theoretically constructive Kripke-semantics in the form of the concrete accessibility relation  ${}_M\mathcal{R}_{\mathbf{CM}}$ ;
  - (b) *parametrically mono-relational*: We may freely choose between the abstract accessibility  ${}_M\mathcal{R}_{\mathbf{CM}}$  and its concrete exemplification (or realisation)  ${}_M\mathcal{R}_{\mathbf{CM}}$  as the accessibility relation in LliP’s Kripke-semantics, but  ${}_M\mathcal{R}_{\mathbf{CM}}$  has also the property of being a partial order with  $\mathbf{CM}$  designating the communication medium. Hence LliP’s essentially mono-relational models subsume seminal bi-relational models of intuitionistic modal logics [Sim94, Page 59] by absorbing the partial order  ${}_M\mathcal{R}_{\mathbf{CM}}$  for the Kripke-semantics of LliP’s intuitionistic connectives as a mere instance of the accessibility relation  ${}_M\mathcal{R}_{\mathbf{CM}}$  for the Kripke-semantics of LliP’s proof modality, thanks to being parametric (and thus generic).
3. We prove a *modal-depth result* applying both to LliP’s necessity as well as its corresponding possibility modality (cf. Corollary 3).
  4. We prove that our  $\mathbf{CM}$ -centred notion of proof is also a *disjunctive explicit* refinement of standard KD45-belief, and yields also such a refinement of standard S5-knowledge and S4-provability (cf. Corollary 5 and 6).
  5. We prove the *finite-model property* (cf. Theorem 4) and therefrom the *algorithmic decidability* of LliP (cf. Corollary 7).

As a side-effect of our work on LliP, we offer an internalised, three-line two-axiom proof of the Disjunction Property of Intuitionistic Logic (IL) originally proved by Gödel. The two axioms are modal internalisations of two fundamental properties of IL, namely the truthfulness of its proofs and Kripke’s Monotonicity Lemma for his semantics of IL. Surprisingly, they jointly trivialise the corresponding box modality ‘ $\Box$ ’ (though *not* the one of LliP) in a technical sense, and thus also, in a non-technical sense, Gödel’s (non-trivial) proof of IL’s Disjunction Property. The truthfulness of intuitionistic proofs corresponds to the well-known modal T-law  $\Box\phi \rightarrow \phi$  and Kripke’s Monotonicity Lemma to the law  $\phi \rightarrow \Box\phi$  (not to be confused with the mentioned monotonicity of proof terms, cf. Page 4 and Remark 1). Jointly, they imply  $\Box(\phi \vee \varphi) \rightarrow (\Box\phi \vee \Box\varphi)$  in any modal logic:

1.  $\vdash \Box(\phi \vee \varphi) \rightarrow (\phi \vee \varphi)$  T

2.  $\vdash (\phi \vee \varphi) \rightarrow (\Box\phi \vee \Box\varphi)$   $\vdash \phi \rightarrow \Box\phi, \vdash \varphi \rightarrow \Box\varphi, \text{IL}$
3.  $\vdash \Box(\phi \vee \varphi) \rightarrow (\Box\phi \vee \Box\varphi)$  1, 2, IL.

### 1.3 Roadmap

In the next section, we introduce our Logic of Intuitionistic interactive Proofs (LIiP) axiomatically by means of a compact closure operator that induces the Hilbert-style proof system that we seek. We then prove a substantial number of useful, deducible structural and logical laws (cf. Theorem 1 and 2) within the obtained system, and therefrom important corollaries (Corollary 2–6), some of which count as our aforementioned contributions in this paper. Next, we introduce the concretely constructed semantics as well as the standard abstract semantic interface for LIiP (cf. Section 2.2), and prove the axiomatic adequacy of the proof system with respect to this interface (cf. Theorem 3). In the construction of the semantics, we again make use of a closure operator, but this time on sets of proof terms. Finally, we prove the finite-model property (cf. Theorem 4) and the algorithmic decidability (cf. Corollary 7) of LDiiP.

## 2 LIiP

### 2.1 Syntactically

The Logic of Intuitionistic interactive Proofs (LIiP) provides a modal *formula language* over a generic message *term language*. The formula language offers the propositional constructors, a relational symbol ‘ $k$ ’ for constructing atomic propositions about so-called individual knowledge (e.g.,  $a k M$ ), and a modal constructor ‘ $\pm$ ’ for propositions about proofs (e.g.,  $M \pm_{\text{cm}} \phi$ ). The message language offers a term constructor for message *pairing* and can accommodate arbitrary other term constructors, e.g., for cryptography (cf. [Kra12a]). The single term constructor of pairing is sufficient for internalising *modus ponens* into the message language (cf. Theorem 2.1) and thus for internalising the single deduction rule of intuitionistic logic into it. *Modus ponens* can be regarded as a minimal requirement for a system to count as a proof system. And so in the context of LIiP, all other term constructors can be regarded as application-specific, and LIiP-theories with such constructors as applied LIiP-theories. These however are not the subject matter of our present paper about basic (or pure) LIiP. (Message signing has no essential role in LIiP as opposed to LiP.) In brief, LIiP is a minimal modular extension of IL with an interactively generalised additional operator (the proof modality) and proof-term language (only one, binary built-in constructor; *agents as proof-checkers*). Alternatively, LIiP can be viewed as a refinement (due to its parameterised modality) and extension (due to additional laws) of Fischer Servi’s [Fis84] or, equivalently, Plotkin and Stirling’s [PS86] basic intuitionistic modal logic IK, promoted in [Sim94] as “the true intuitionistic analogue of K.” See [dPR11] for a recent discussion of this purported truth and alternative contribution in the form of the so-called basic



constructive modal logic CK, which can be embedded into IK [Ran10]. Note that the formula language of LliP is identical to the one of LiP [Kra12a] modulo the term language and the proof-modality notation. The term language of LliP is strictly included in the term language of LiP but may be arbitrarily extended. The proof-modality notation in LliP is ‘ $\pm$ ’ whereas it is ‘ $:$ ’ in LiP.

In the sequel, grey-shading indicates essential differences to LiP.

**Definition 1** (The language of LliP). Let

- $\mathcal{A}$  designate a finite set of *agent names*  $a, b, c$ , etc. such that  $\mathbf{CM} \in \mathcal{A}$ , where  $\mathbf{CM}$  designates the communication medium (admissible also in LiP);
- $\mathcal{M} \ni M ::= a \mid B \mid (M, M)$  designate our language of *message terms*  $M$  over  $\mathcal{A}$  with (transmittable) agent names  $a \in \mathcal{A}$ , application-specific data  $B$  (left blank here), and message-term pairs  $(M, M)$ ;  
(Messages must be grammatically well-formed, which yields an induction principle. So agent names  $a$  are logical term constants, the meta-variable  $B$  just signals the possibility of an extended term language  $\mathcal{M}$ , and  $(\cdot, \cdot)$  is a binary functional symbol. For other term constructors, see [Kra12a].)
- $\mathcal{P}$  designate a denumerable set of *propositional variables*  $P$  constrained such that for all  $a \in \mathcal{A}$  and  $M \in \mathcal{M}$ ,  $(a \mathbf{k} M) \in \mathcal{P}$  (for “ $a$  knows  $M$ ”) is a distinguished variable, i.e., an *atomic proposition*, (for *individual knowledge*); (So, for  $a \in \mathcal{A}$ ,  $a \mathbf{k} \cdot$  is a unary relational symbol.)
- $\mathcal{L} \ni \phi ::= P \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg \phi \mid \phi \rightarrow \phi \mid$   $M \pm_{\mathbf{CM}} \phi$  designate our language of *logical formulas*  $\phi$ , where the modal-necessity formula  $M \pm_{\mathbf{CM}} \phi$  reads as “ $M$  can intuitionistically prove that  $\phi$  (is true) to  $\mathbf{CM}$ .”

Note the following macro-definitions:  $\top := \mathbf{CM} \mathbf{k} \mathbf{CM}$ ,  $\perp := \neg \top$ ,  $\phi \leftrightarrow \phi' := (\phi \rightarrow \phi') \wedge (\phi' \rightarrow \phi)$ ,  $\blacksquare \phi := \mathbf{CM} \pm_{\mathbf{CM}} \phi$  (see also Theorem 2.8),  $\Diamond \phi := \neg \neg \phi$ , and

$M \mp_{\mathbf{CM}} \phi := \Diamond(\mathbf{CM} \mathbf{k} M \wedge \phi)$  (*double negation as modal possibility* rather than necessity, unlike in [Doš84]; see also Theorem 2.58). Recall that whereas conjunction and disjunction connectives as well as necessitation and possibility modalities are dually inter-definable in classical modal logic by means of negation, they are not necessarily so in intuitionistic modal logic [Sim94, Requirement 5]. However, as our above macro-definition of  $M \mp_{\mathbf{CM}} \phi$  in terms of a double negation and individual knowledge foreshadows,  $M \mp_{\mathbf{CM}} \phi$  fortunately is not necessary as a primitive modality in the language of LliP. ([AI07] remain silent as to the dual of their intuitionistic-proof modality.)

Then, LliP has the following axiom and deduction-rule schemas.

**Definition 2** (The axioms and deduction rules of LliP). Let

- $\Gamma_0$  designate an adequate set of axioms for intuitionistic propositional logic
- $\Gamma_1 := \Gamma_0 \cup \{$

- $a \mathbf{k} a$  (knowledge of one's own name string)
- $(a \mathbf{k} M \wedge a \mathbf{k} M') \leftrightarrow a \mathbf{k} (M, M')$  ([un]pairing)
- $M \pm_{\mathbf{CM}} \mathbf{CM} \mathbf{k} M$  (self-knowledge)
- $(M \pm_{\mathbf{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \pm_{\mathbf{CM}} \phi) \rightarrow M \pm_{\mathbf{CM}} \phi')$  (K)
- $(M \pm_{\mathbf{CM}} \phi) \rightarrow (\mathbf{CM} \mathbf{k} M \rightarrow \phi)$  (epistemic T, ET)
- $(M \pm_{\mathbf{CM}} \phi) \rightarrow M \mp_{\mathbf{CM}} \phi$  (intuitionistic D, ID)
- $\phi \rightarrow M \pm_{\mathbf{CM}} \phi$  (modal monotonicity, MM) }

designate a set of *axiom schemas*.

Then,  $\mathbf{LLiP} := \mathbf{Cl}(\emptyset) := \bigcup_{n \in \mathbb{N}} \mathbf{Cl}^n(\emptyset)$ , where for all  $\Gamma \subseteq \mathcal{L}$ :

$$\begin{aligned}
\mathbf{Cl}^0(\Gamma) &:= \Gamma_1 \cup \Gamma \\
\mathbf{Cl}^{n+1}(\Gamma) &:= \mathbf{Cl}^n(\Gamma) \cup \\
&\quad \{ \phi' \mid \{ \phi, \phi \rightarrow \phi' \} \subseteq \mathbf{Cl}^n(\Gamma) \} \cup \quad (\textit{modus ponens}, \text{MP}) \\
&\quad \{ (M' \pm_{\mathbf{CM}} \phi) \rightarrow M \pm_{\mathbf{CM}} \phi \mid (\mathbf{CM} \mathbf{k} M \rightarrow \mathbf{CM} \mathbf{k} M') \in \mathbf{Cl}^n(\Gamma) \} \\
&\quad (\textit{epistemic antitonicity}, \text{EA}).
\end{aligned}$$

We call  $\mathbf{LLiP}$  a *base theory*, and  $\mathbf{Cl}(\Gamma)$  an *LLiP-theory* for any  $\Gamma \subseteq \mathcal{L}$ .

Notice the logical order of  $\mathbf{LLiP}$ , which like  $\mathbf{LiP}$ 's is, due to propositions about (proofs of) propositions, *higher-order propositional*.

**Inherited laws** From  $\mathbf{LiP}$  [Kra12a], we recall the discussion of the (un)pairing axiom, Kripke's law (K), the laws of epistemic T (ET) and epistemic antitonicity (EA): We assume the existence of a pairing mechanism modelling finite sets. Such a mechanism is required by the important application of communication (not only cryptographic) protocols [And08, Chapter 3], in which concatenation of high-level data packets is associative, commutative, and idempotent. The key to the validity of K is that we understand interactive proofs as sufficient evidence for intended resource-unbounded proof-checking agents (who are though still unable to guess). Clearly for such agents, if  $M$  is sufficient evidence for  $\phi \rightarrow \phi'$  and  $\phi$  then so is  $M$  for  $\phi'$ . Then, the significance of ET (which as opposed to the standard T-law is conditioned on individual knowledge) to interactivity is that in truly distributed multi-agent systems, not all proofs are known by all agents, i.e., agents are not omniscient with respect to messages. Otherwise, why communicate with each other? So there being a proof does not imply knowledge of that proof. When an agent  $a$  does not know the proof and the agent cannot generate the proof *ex nihilo* herself by guessing it, only communication from a peer, who thus acts as an oracle, can entail the knowledge of the proof with  $a$ . Finally, note that the law of self-knowledge is a theorem but not an axiom in  $\mathbf{LiP}$ , and observe that EA is a rule of *logical modularity* that allows the modular generation of structural modal laws from implication term laws (cf. Theorem 1).

**New laws** We continue to discuss the new laws of LliP, which are all axiom schemas: In contrast to LiP [Kra12a], LliP must have an *intuitionistic* rather than a classical propositional axiom base  $\Gamma_0$  as already explained at the end of Section 1.1.1. Next, ID says that intuitionistic necessity (“box”) implies intuitionistic possibility (“diamond”). As opposed to its classical-modal-logic equivalent D, ID cannot be alternatively stated in the shape of  $\vdash \Box\phi \rightarrow \neg\Box\neg\phi$ . Then, the law of modal monotonicity MM reflects the semantic fact mentioned in Section 1.2 that LliP’s Kripke-model absorbs the partial order for the Kripke-semantics of LliP’s intuitionistic connectives as a mere instance of the accessibility relation for the Kripke-semantics of LliP’s proof modality, thanks to being parametric (and thus generic, cf. Section 2.2). Thus we adopt formulas of the shape  $\phi \rightarrow \Box\phi$  as axioms MM in our intuitionistic modal logical system LliP, like Došen in his intuitionistic modal logical system *Hdn* $\Box$  [Doš84], where he adopts formulas of that form as axioms *dn2*. To our knowledge, *Hdn* $\Box$  and LliP are the only intuitionistic modal logics with such axioms. Finally, we could add admissible but not derivable rules and their corresponding internalising axioms to LliP in the style of [AI07]. (Recall from [Mos10] that the admissible rules of a theory are the rules under which the theory is closed. Hence the set of primitive and derivable rules is a subset of the set of admissible rules, and [but not] vice versa in classical [intuitionistic] logic. [IL is *structurally incomplete*.] See [Jeř08] for suitable *bases* of admissible rules.) However, since the addition of admissible but not derivable rules to a theory does not change the theory, such an addition can be considered as unnecessary, at least in our base theory.

In the sequel, “:iff” abbreviates “by definition, if and only if”.

**Proposition 1** (Hilbert-style proof system). *Let*

- $\Phi \vdash_{\text{LliP}} \phi$  :iff if  $\Phi \subseteq \text{LliP}$  then  $\phi \in \text{LliP}$
- $\phi \dashv\vdash_{\text{LliP}} \phi'$  :iff  $\{\phi\} \vdash_{\text{LliP}} \phi'$  and  $\{\phi'\} \vdash_{\text{LliP}} \phi$
- $\vdash_{\text{LliP}} \phi$  :iff  $\emptyset \vdash_{\text{LliP}} \phi$ .

In other words,  $\vdash_{\text{LliP}} \subseteq 2^{\mathcal{L}} \times \mathcal{L}$  is a system of closure conditions in the sense of [Tay99, Definition 3.7.4]. For example:

1. for all axioms  $\phi \in \Gamma_1$ ,  $\vdash_{\text{LliP}} \phi$
2. for modus ponens,  $\{\phi, \phi \rightarrow \phi'\} \vdash_{\text{LliP}} \phi'$
3. for epistemic antitonicity,
 
$$\{\text{CM } k M \rightarrow \text{CM } k M'\} \vdash_{\text{LliP}} (M' \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi.$$

(In the space-saving, horizontal Hilbert-notation “ $\Phi \vdash_{\text{LliP}} \phi$ ”,  $\Phi$  is not a set of hypotheses but a set of premises, cf. modus ponens and epistemic antitonicity.)

Then,  $\vdash_{\text{LliP}}$  can be viewed as being defined by a Cl-induced Hilbert-style proof system. In fact  $\text{Cl} : 2^{\mathcal{L}} \rightarrow 2^{\mathcal{L}}$  is a standard consequence operator, i.e., a substitution-invariant compact closure operator.

*Proof.* Like in [Kra12a]. That a Hilbert-style proof system can be viewed as induced by a compact closure operator is well-known (e.g., see [Gab95]); that  $\text{Cl}$  is indeed such an operator can be verified by inspection of the inductive definition of  $\text{Cl}$ ; and substitution invariance follows from our definitional use of axiom *schemas*.<sup>4</sup>  $\square$

**Corollary 1** (Normality). *LIIP is a normal modal logic.*

*Proof.* Jointly by Kripke’s law and *modus ponens* (by definition), necessitation (cf. proof of Theorem 2.0), and substitution invariance (cf. Proposition 1).  $\square$

We are now going to present some useful deducible *structural* laws of LIIP, including the deducible non-structural rule of epistemic bitonicity, used in the deduction of some of them. Here, “structural” means “deducible exclusively from term axioms.” The laws are enumerated in a (total) order that respects (but cannot reflect) their respective proof prerequisites. The laws are also deducible in LiP, in the same order and without non-intuitionistic machinery [Kra12a].

**Theorem 1** (Some useful deducible structural laws).

1.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, M') \rightarrow a \mathbf{k} M$   
(left projection, 1-way K-combinator property)
2.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, M') \rightarrow a \mathbf{k} M'$  (right projection)
3.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, M) \leftrightarrow a \mathbf{k} M$  (pairing idempotency)
4.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, M') \leftrightarrow a \mathbf{k} (M', M)$  (pairing commutativity)
5.  $\vdash_{\text{LIIP}} (a \mathbf{k} M \rightarrow a \mathbf{k} M') \leftrightarrow (a \mathbf{k} (M, M') \leftrightarrow a \mathbf{k} M)$   
(neutral pair elements)
6.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, a) \leftrightarrow a \mathbf{k} M$  (self-neutral pair element)
7.  $\vdash_{\text{LIIP}} a \mathbf{k} (M, (M', M'')) \leftrightarrow a \mathbf{k} ((M, M'), M'')$  (pairing associativity)
8.  $\{\mathbf{CM} \mathbf{k} M \leftrightarrow \mathbf{CM} \mathbf{k} M'\} \vdash_{\text{LIIP}} (M \pm_{\mathbf{CM}} \phi) \leftrightarrow M' \pm_{\mathbf{CM}} \phi$  (epistemic bitonicity)
9.  $\vdash_{\text{LIIP}} (M \pm_{\mathbf{CM}} \phi) \rightarrow (M', M) \pm_{\mathbf{CM}} \phi$  (proof extension, left)
10.  $\vdash_{\text{LIIP}} (M \pm_{\mathbf{CM}} \phi) \rightarrow (M, M') \pm_{\mathbf{CM}} \phi$  (proof extension, right)
11.  $\vdash_{\text{LIIP}} ((M \pm_{\mathbf{CM}} \phi) \vee M' \pm_{\mathbf{CM}} \phi) \rightarrow (M, M') \pm_{\mathbf{CM}} \phi$  (proof extension)
12.  $\vdash_{\text{LIIP}} ((M, M) \pm_{\mathbf{CM}} \phi) \leftrightarrow M \pm_{\mathbf{CM}} \phi$  (proof idempotency)
13.  $\vdash_{\text{LIIP}} ((M, M') \pm_{\mathbf{CM}} \phi) \leftrightarrow (M', M) \pm_{\mathbf{CM}} \phi$  (proof commutativity)
14.  $\{\mathbf{CM} \mathbf{k} M \rightarrow \mathbf{CM} \mathbf{k} M'\} \vdash_{\text{LIIP}} ((M, M') \pm_{\mathbf{CM}} \phi) \leftrightarrow M \pm_{\mathbf{CM}} \phi$   
(neutral proof elements)

<sup>4</sup>Alternatively to axiom schemas, we could have used axioms together with an additional substitution-rule set  $\{ \sigma[\phi] \mid \phi \in \text{Cl}^n(\Gamma) \}$  in the definiens of  $\text{Cl}^{n+1}(\Gamma)$ .

15.  $\vdash_{\text{LiP}} ((M, \text{CM}) \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi$  (*self-neutral proof element*)

16.  $\vdash_{\text{LiP}} ((M, (M', M'')) \pm_{\text{CM}} \phi) \leftrightarrow ((M, M'), M'') \pm_{\text{CM}} \phi$   
(*proof associativity*)

*Proof.* Like in [Kra12a]—no non-intuitionistic machinery is required.  $\square$

For a discussion of these LiP laws, consider our discussion of their analogs in LiP [Kra12a] and the following remark.

**Remark 1** (Monotonicity—Proof & Truth). The law of proof extension captures the monotonicity of the *proof terms* in LiP mentioned in Table 1, as does its analog in LiP. In contrast, the law of modal monotonicity (cf. Definition 2), which does not hold in LiP, captures the monotonicity of the *local truths* in LiP. Recall from Section 1 that in an intuitionistic (modal) universe (such as LiP’s), all, i.e., positive or negative (whence the notation ‘ $\pm_{\text{CM}}$ ’), (local) truths are monotonic. Whereas in a classical (modal) universe (such as LiP’s), not all (local) truths need be monotonic. If a proof term is monotonic then its proof goal is. If a proof goal is monotonic then its proof must be. In LiP, all proof goals are monotonic, thanks to LiP being intuitionistic, which is what forces them to be so. However in LiP, not all proof goals need be monotonic, because of LiP being classical as well as modal, which is what frees them from being so.

**Corollary 2** (S-combinator property).

1.  $\vdash_{\text{LiP}} a k ((M, M'), M'') \leftrightarrow a k (M, (M'', (M', M'')))$

2.  $\vdash_{\text{LiP}} (((M, M'), M'') \pm_{\text{CM}} \phi) \leftrightarrow (M, (M'', (M', M''))) \pm_{\text{CM}} \phi$

*Proof.* Like in [Kra12a]—again, no non-intuitionistic machinery is required.  $\square$

We are going to present also some useful, deducible *logical* laws of LiP. Here, “logical” means “not structural” in the previously defined sense. Also these laws are enumerated in an order that respects their respective proof prerequisites. Grey-shading indicates special interest for intuitionistic modal logic in general and for LiP as opposed to (the classical) LiP in particular. Three important themes therein are: first, intuitionistic negation (single ‘ $\neg$ ’ and double ‘ $\neg\neg$ ’) and second, individual knowledge ( $\text{CM} k M$ ), and their import for the relation between  $M \pm_{\text{CM}} \phi$  and its dual  $M \mp_{\text{CM}} \phi$ , which is normally not one of identity nor dual definability in intuitionistic modal logic; and third, the internalised disjunction property (IDP), which does not hold in LiP. ([AI07] remain silent about the deducibility of an IDP in their logic, which, given that they internalise standard IL, is intriguing.) Theorem 2 has four important corollaries, among which there is a modal-depth result, the relation of LiP to Fischer Servi’s [Fis84] and Plotkin and Stirling’s [PS86] seminal work on intuitionistic modal logic, and the relation of LiP to standard doxastic [MV07] and epistemic logic [MV07, FHMV95, HR10]. The number of intermediate results required to obtain the corollaries, reflected in the length of Theorem 2, may be indicative of the exponential blow-up in proof length of intuitionistic over classical logic

[Hru07]. The non-intuitionistically inclined reader may want to skip them except Theorem 2.58. Whereas the intuitionistically inclined reader may want to prove them herself, in order and as milestones for proving their corollaries.

**Theorem 2** (Some useful deducible logical laws).

0.  $\{\phi\} \vdash_{\text{LHP}} M \pm_{\text{CM}} \phi$  (*necessitation, N*)
1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow ((M' \pm_{\text{CM}} \phi) \rightarrow (M, M') \pm_{\text{CM}} \phi')$   
(*generalised Kripke-law, GK*)
2.  $\{\phi \rightarrow \phi'\} \vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi'$  (*regularity, R*)
3.  $\{\phi \leftrightarrow \phi'\} \vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi'$  (*R bis*)
4.  $\{\text{CM k } M \rightarrow \text{CM k } M', \phi \rightarrow \phi'\} \vdash_{\text{LHP}} (M' \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi'$   
(*epistemic regularity, ER*)
5.  $\{\text{CM k } M \leftrightarrow \text{CM k } M', \phi \leftrightarrow \phi'\} \vdash_{\text{LHP}} (M' \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi'$  (*ER bis*)
6.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} \top$  (*anything can prove tautological truth*)
7.  $\vdash_{\text{LHP}} M \mp_{\text{CM}} \top$  (*anything can disprove tautological falsehood*)
8.  $\vdash_{\text{LHP}} \blacksquare \phi \leftrightarrow \phi$  (*TMM*)
9.  $\phi \dashv\vdash_{\text{LHP}} \blacksquare \phi$  (*TMM bis*)
10.  $\vdash_{\text{LHP}} \text{CM k } M \rightarrow ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  (*ET bis*)
11.  $\vdash_{\text{LHP}} \neg \neg (\text{CM k } M)$  (*CM message communicability, CMMC*)
12.  $\vdash_{\text{LHP}} \neg \neg ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  (*possible TMM, PTMM*)
13.  $\vdash_{\text{LHP}} \neg \phi \rightarrow \neg (M \mp_{\text{CM}} \phi)$   
(*falsehood implies falsehood non-disprovability, FIFND*)
14.  $\vdash_{\text{LHP}} \neg (M \mp_{\text{CM}} \phi) \leftrightarrow \neg (M \pm_{\text{CM}} \phi)$   
(*falsehood non-disprovability equals truth unprovability, FNDETU*)
15.  $\vdash_{\text{LHP}} \neg \phi \rightarrow \neg (M \pm_{\text{CM}} \phi)$   
(*falsehood implies truth unprovability, FITU*)
16.  $\vdash_{\text{LHP}} \neg \neg \phi \rightarrow \neg (M \mp_{\text{CM}} \neg \phi)$  (*FIFND bis*)
17.  $\vdash_{\text{LHP}} \neg (M \mp_{\text{CM}} \neg \phi) \leftrightarrow \neg (M \pm_{\text{CM}} \neg \phi)$  (*FNDETU bis*)
18.  $\vdash_{\text{LHP}} \neg \neg \phi \rightarrow \neg (M \pm_{\text{CM}} \neg \phi)$  (*FITU bis*)

19.  $\vdash_{\text{LHP}} (\phi \vee (M \pm_{\text{CM}} \phi) \vee M \mp_{\text{CM}} \phi) \rightarrow$   
 $(\neg\neg\phi \wedge \neg(M \mp_{\text{CM}} \neg\phi) \wedge \neg(M \pm_{\text{CM}} \neg\phi))$   
*(extended weak double-negation law, EWDN)*
20.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi') \rightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi')$   
*(conditional functionality, CF)*
21.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi) \rightarrow ((M \mp_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi)$   
*(local classicality implies modal equivalence, LCIME)*
22.  $\vdash_{\text{LHP}} (\text{CM k } M \wedge M \pm_{\text{CM}} \phi) \rightarrow (\neg\neg\phi \rightarrow \phi)$   
*(proof knowledge implies local classicality, PKILC)*
23.  $\vdash_{\text{LHP}} (\text{CM k } M \wedge M \pm_{\text{CM}} \phi) \rightarrow ((M \mp_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi)$   
*(proof knowledge implies modal equivalence, PKIME)*
24.  $\vdash_{\text{LHP}} \neg(M \pm_{\text{CM}} \perp)$  *(nothing can prove tautological falsehood)*
25.  $\vdash_{\text{LHP}} \neg(M \mp_{\text{CM}} \perp)$  *(nothing can disprove tautological truth)*
26.  $\vdash_{\text{LHP}} \phi \rightarrow M \mp_{\text{CM}} \phi$  *(weak MM, WMM)*
27.  $\{\text{CM k } M \rightarrow \phi\} \Vdash_{\text{LHP}} M \pm_{\text{CM}} \phi$  *(epistemic N, EN)*
28.  $\{\text{CM k } M \rightarrow \text{CM k } M'\} \Vdash_{\text{LHP}} M \pm_{\text{CM}} \text{CM k } M'$  *(EN bis)*
29.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  *(ET bis self-proof)*
30.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)$  *(4)*
31.  $\vdash_{\text{LHP}} \neg(M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \neg(M \pm_{\text{CM}} \phi)$  *(5)*
32.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \wedge M' \pm_{\text{CM}} \phi') \rightarrow (M, M') \pm_{\text{CM}} (\phi \wedge \phi')$   
*(proof conjunctions)*
33.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \wedge M' \pm_{\text{CM}} \phi') \leftrightarrow M \pm_{\text{CM}} (\phi \wedge \phi')$  *(proof conjunctions bis)*
34.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \vee M' \pm_{\text{CM}} \phi') \rightarrow (M, M') \pm_{\text{CM}} (\phi \vee \phi')$  *(proof disjunctions)*
35.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \vee M' \pm_{\text{CM}} \phi') \rightarrow M \pm_{\text{CM}} (\phi \vee \phi')$  *(proof disjunctions bis)*
36.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \leftrightarrow M \pm_{\text{CM}} \phi$  *(modal idempotency, MI)*
37.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow M \mp_{\text{CM}} \phi$  *(MI bis)*
38.  $\vdash_{\text{LHP}} (\phi \vee (M \pm_{\text{CM}} \phi) \vee M \mp_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi)$   
*(nested MM, NMM)*
39.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi)$  *(modal swap, MS)*

40.  $\vdash_{\text{LHP}} \mathbf{CM} \mathbf{k} M \rightarrow ((M \pm_{\mathbf{CM}} (\phi \vee \phi')) \rightarrow ((M \pm_{\mathbf{CM}} \phi) \vee M \pm_{\mathbf{CM}} \phi'))$   
(*epistemic internalised disjunction property, EIDP*)
41.  $\vdash_{\text{LHP}} M \pm_{\mathbf{CM}} ((M \pm_{\mathbf{CM}} (\phi \vee \phi')) \rightarrow ((M \pm_{\mathbf{CM}} \phi) \vee M \pm_{\mathbf{CM}} \phi'))$   
(*IDP self-proof*)
42.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} \phi) \leftrightarrow M \pm_{\mathbf{CM}} (\mathbf{CM} \mathbf{k} M \wedge \phi)$  (*epistemic idempotency, EI*)
43.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} \phi) \leftrightarrow M \pm_{\mathbf{CM}} (\mathbf{CM} \mathbf{k} M \wedge M \pm_{\mathbf{CM}} \phi)$  (*EI bis*)
44.  $\vdash_{\text{LHP}} (M \mp_{\mathbf{CM}} (\phi \vee \phi')) \leftrightarrow ((M \mp_{\mathbf{CM}} \phi) \vee M \mp_{\mathbf{CM}} \phi')$   
(*Plotkin-Stirling 4, PS4*)
45.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \mp_{\mathbf{CM}} \phi) \rightarrow M \mp_{\mathbf{CM}} \phi')$   
(*Plotkin-Stirling 2, PS2*)
46.  $\vdash_{\text{LHP}} ((M \mp_{\mathbf{CM}} \phi) \rightarrow M \pm_{\mathbf{CM}} \phi') \rightarrow M \pm_{\mathbf{CM}} (\phi \rightarrow \phi')$   
(*Plotkin-Stirling 5, PS5*)
47.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi') \rightarrow M \pm_{\mathbf{CM}} (\phi \rightarrow \phi')$  (*CFPS5*)
48.  $\vdash_{\text{LHP}} ((\neg\neg\phi \rightarrow \phi') \wedge (\neg\neg\phi' \rightarrow \phi)) \rightarrow$   
 $((M \pm_{\mathbf{CM}} (\phi \vee \phi')) \rightarrow ((M \pm_{\mathbf{CM}} \phi) \vee M \pm_{\mathbf{CM}} \phi'))$   
(*conditional IDP, CIDP*)
49.  $\vdash_{\text{LHP}} (\phi \vee (M \pm_{\mathbf{CM}} \phi) \vee M \mp_{\mathbf{CM}} \phi) \rightarrow M \pm_{\mathbf{CM}} (M \mp_{\mathbf{CM}} \phi)$  (*NMM bis*)
50.  $\vdash_{\text{LHP}} (M \mp_{\mathbf{CM}} (M \pm_{\mathbf{CM}} \phi)) \rightarrow M \pm_{\mathbf{CM}} (M \mp_{\mathbf{CM}} \phi)$  (*MS bis*)
51.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} (M \mp_{\mathbf{CM}} \phi)) \leftrightarrow M \mp_{\mathbf{CM}} (M \pm_{\mathbf{CM}} \phi)$   
(*modal commutativity, MC*)
52.  $\vdash_{\text{LHP}} (M \mp_{\mathbf{CM}} (M \pm_{\mathbf{CM}} \phi)) \leftrightarrow M \mp_{\mathbf{CM}} \phi$   
(*mixed modal idempotency, MMI*)
53.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} (M \mp_{\mathbf{CM}} \phi)) \leftrightarrow M \mp_{\mathbf{CM}} \phi$  (*MMI bis*)
54.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} \neg\neg\phi) \rightarrow M \mp_{\mathbf{CM}} \phi$  (*double-negation absorption, DNA*)
55.  $\vdash_{\text{LHP}} (M \pm_{\mathbf{CM}} \neg\neg\phi) \rightarrow \neg\neg(M \pm_{\mathbf{CM}} \phi)$  (*double-negation extrusion, DNE*)
56.  $\vdash_{\text{LHP}} \neg(M \mp_{\mathbf{CM}} \phi) \rightarrow M \mp_{\mathbf{CM}} \neg\phi$  (*weak negation completeness, WNC*)
57.  $\vdash_{\text{LHP}} \neg(M \pm_{\mathbf{CM}} \phi) \rightarrow M \mp_{\mathbf{CM}} \neg\phi$  (*WNC bis*)



$$58. \quad \boxed{\vdash_{\text{LiP}} (M \mp_{\text{CM}} \phi) \leftrightarrow \neg \neg (M \pm_{\text{CM}} \phi)} \quad (\text{modal double negation, MDN})$$

$$59. \quad \vdash_{\text{LiP}} ((M \pm_{\text{CM}} \phi) \wedge M \mp_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow M \mp_{\text{CM}} \phi \quad (Wiv)$$

$$60. \quad \vdash_{\text{LiP}} (M \mp_{\text{CM}} (\phi \wedge \neg \phi')) \rightarrow (\phi \wedge \neg \phi') \quad (Wv)$$

*Proof.* See Appendix A.1. □

The following remark flags a non-trivial insight, also explicated in Section 2.2.

**Remark 2** (Intuitionistic truths). Theorem 2.8 means that in interactive settings, the intuitionistic truths are those of the communication medium.

The reader is invited to compare Theorem 2.8 to its global counterpart Theorem 2.27, whose analog also holds in LiP but was not stated there.

**Corollary 3** (Modal-depth result). *Let  $\heartsuit_1 \cdots \heartsuit_n \phi \in \mathcal{L}$  such that for all  $1 \leq i \leq n$ ,  $\heartsuit_i \in \{M \pm_{\text{CM}}, M \mp_{\text{CM}}\}$ . Then, if the prefix ' $\heartsuit_1 \cdots \heartsuit_n$ ' contains*

*1. only occurrences of the ' $M \pm_{\text{CM}}$ '-modality then*

$$\vdash_{\text{LiP}} (\heartsuit_1 \cdots \heartsuit_n \phi) \leftrightarrow M \pm_{\text{CM}} \phi;$$

*2. at least one occurrence of the ' $M \mp_{\text{CM}}$ '-modality then*

$$\vdash_{\text{LiP}} (\heartsuit_1 \cdots \heartsuit_n \phi) \leftrightarrow M \mp_{\text{CM}} \phi.$$

*Proof.* For 1, apply MI. For 2, apply MI, MI bis, MMI, and MMI bis. □

**Corollary 4** (Intuitionistic Modal Logic). *LiP is a refinement (due to its parameterised modality) and extension (due to additional laws) of Fischer Servi's [Fis84] and Plotkin and Stirling's [PS86] intuitionistic modal logic IK.*

*Similarly is LiP a refinement and extension of the propositional fragment of Wijesekera's system of first-order constructive modal logic [Wij90, Section 1.5].*

*Proof.* In fact, Plotkin and Stirling's axiomatisation of IK, which is equivalent to Fischer Servi's, consists of the axioms of IL and the laws K, MP, N as well as the axiom analogs of Theorem 2.25 and 2.44–2.46; and the propositional fragment of Wijesekera's system consists of the axioms of IL and the laws K, MP, N as well as the axiom analogs of Theorem 2.45, 2.59 and 2.60. □

The following corollary asserts that our disjunctive proof modality is also an *explicit refinement* of the standard (implicit) belief modality [MV07].

**Corollary 5** (Disjunctive Explicit Belief). *' $M \pm_{\text{CM}} \cdot$ ' is a disjunctive KD45-modality of explicit agent belief, where  $M$  represents the explicit evidence term that can justify the agent CM's belief. Additionally, the communication medium CM is a truth-believing agent in the sense that  $\vdash_{\text{LiP}} \phi \rightarrow M \pm_{\text{CM}} \phi$ .*

*Proof.* Consider that ' $M \pm_{\text{CM}} \cdot$ ' satisfies the K-law (cf. Definition 2), the D-law (called ID in Definition 2), the 4-law (cf. Theorem 2.30), the 5-law (cf. Theorem 2.31), IDP self-proof (cf. Theorem 2.41), the MM-law (cf. Definition 2), and the N-law (cf. Theorem 2.0).  $\square$

Thanks to Theorem 2.10,  $\text{CM} \mathbf{k} M$  is a sufficient condition for ' $M \pm_{\text{CM}} \cdot$ ' to behave like a standard S5-modality of *perfect knowledge* (in a technical sense) [MV07, FHMV95, HR10], which in addition to being a KD45-modality not only obeys the D-law but also the stronger T-law (knowledge, not only belief) and the MM-law (*perfect knowledge*):

$$\vdash_{\text{LIP}} \text{CM} \mathbf{k} M \rightarrow ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi).$$

**Remark 3** (Perfect knowledge). In interactive settings, only the communication medium  $\text{CM}$ , through which all messages have to pass, can attain perfect knowledge (the other agents having only partial visibility of the network, cf. Definition 3). However note that LIP being propositionally modal-intuitionistic, this perfect knowledge is of propositional invariants of the communication network only (cf. Page 4). So the epistemic perfection of the communication medium is only within a certain *grain* (propositional) and *scope* (invariants).

In the following corollary, we construct also a disjunctive explicit refinement of (implicit) S4-provability.

**Corollary 6** (Disjunctive Explicit Provability). ' $\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} \cdot$ ' is a disjunctive S4-modality of *explicit agent provability*, where  $M$  represents the *explicit evidence term that does justify agent CM's knowledge*.

*Proof.* By Corollary 5, Theorem 2.10, and Theorem 2.40: The T-law  $\vdash_{\text{LDIP}} (\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} \phi) \rightarrow \phi$  for the modality ' $\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} \cdot$ ' can be recognised by inspecting Theorem 2.10, and the disjunctivity  $\vdash_{\text{LDIP}} (\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} (\phi \vee \phi')) \rightarrow ((\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} \phi) \vee (\text{CM} \mathbf{k} M \wedge M \pm_{\text{CM}} \phi'))$  by inspecting Theorem 2.40.  $\square$

## 2.2 Semantically

We continue to present the concretely constructed semantics as well as the standard abstract semantic interface for LIP, and prove the axiomatic adequacy of the proof system with respect to this interface. The core ingredient of the concrete semantics of LIP are so-called *input histories*, which were introduced in [Kra12b, Kra13b] and could also be used in an even more concrete semantics of LiP. Input histories are finite words of input events and serve as concrete states  $s \in \mathcal{S}$  in the state space  $\mathcal{S}$ , on which the concrete and abstract accessibility relation  ${}_M \mathbf{R}_{\text{CM}} \subseteq \mathcal{S} \times \mathcal{S}$  and  ${}_M \mathbf{R}_{\text{CM}} \subseteq \mathcal{S} \times \mathcal{S}$  for LIP is defined, respectively. The reader of [Kra12a, Kra13c] will recognise similar but simpler definitions here; the one of  ${}_M \mathbf{R}_{\text{CM}}$  could be even simpler (cf. Fact 1.2), but is as now in order to allow for a simpler, pattern-matching comparison with the corresponding one in [Kra12a, Kra13c]. (We wanted to show how to produce LIP from LiP.)

### 2.2.1 Concretely

**Definition 3** (Semantic ingredients). For the set-theoretically constructive, model-theoretic study of LliP let

- $\mathcal{S} \ni s ::= 0 \mid \text{succ}_a^M(s)$  designate the concrete state space  $\mathcal{S}$  of *input histories*  $s$ , where  $0$  designates the empty input history (i.e., a zero data point, e.g., an initial state) and  $\text{succ}_a^M$  can be read as “agent  $a$  receives message  $M$ ” (e.g., from some other agent acting as an oracle for  $a$ ); and  $\star : (\mathcal{S} \times \mathcal{S}) \rightarrow \mathcal{S}$  monoidal concatenation on  $\mathcal{S}$  (with neutral element  $0$ );
- $\pi_a : \mathcal{S} \rightarrow \mathcal{S}$  designate (local) *state projection on  $a$ ’s view* such that

$$\begin{aligned} \pi_a(0) &:= 0 \\ \pi_a(\text{succ}_b^M(s)) &:= \begin{cases} \text{succ}_b^M(\pi_a(s)) & \text{if } a \in \{b, \text{CM}\}, \text{ and} \\ \pi_a(s) & \text{otherwise;} \end{cases} \end{aligned}$$

(The communication medium **CM** sees any agent’s  $b$  [including its own] input events, i.e., **CM** has a global view on the current global state  $s$ .)

- $\text{msgs} : \mathcal{S} \rightarrow 2^{\mathcal{M}}$  designate *raw-data extraction* such that

$$\begin{aligned} \text{msgs}(0) &:= \emptyset \\ \text{msgs}(\text{succ}_a^M(s)) &:= \text{msgs}(s) \cup \{M\}; \end{aligned}$$

- $\text{msgs}_a := \text{msgs} \circ \pi_a$  designate (local) *raw-data extraction by  $a$* ;
- $\text{cl}_a^s : 2^{\mathcal{M}} \rightarrow 2^{\mathcal{M}}$  designate a *data-mining operator* such that  $\text{cl}_a^s(\mathcal{D}) := \text{cl}_a(\text{msgs}_a(s) \cup \mathcal{D}) := \bigcup_{n \in \mathbb{N}} \text{cl}_a^n(\text{msgs}_a(s) \cup \mathcal{D})$ , where for all  $\mathcal{D} \subseteq \mathcal{M}$ :

$$\begin{aligned} \text{cl}_a^0(\mathcal{D}) &:= \{a\} \cup \mathcal{D} \\ \text{cl}_a^{n+1}(\mathcal{D}) &:= \text{cl}_a^n(\mathcal{D}) \cup \\ &\quad \{ (M, M') \mid \{M, M'\} \subseteq \text{cl}_a^n(\mathcal{D}) \} \cup \quad (\text{pairing}) \\ &\quad \{ M, M' \mid (M, M') \in \text{cl}_a^n(\mathcal{D}) \} \quad (\text{unpairing}) \end{aligned}$$

( $\text{cl}_a^s(\emptyset)$  can be viewed as  $a$ ’s *individual-knowledge base* in  $s$ . For application-specific terms such as signing and encryption, we would have to add here the closure conditions corresponding to their characteristic term axioms.)

- $\sqsubseteq_a \subseteq \mathcal{S} \times \mathcal{S}$  designate the (local) *state **pre-order** of  $a$*  such that for all  $s, s' \in \mathcal{S}$ ,  $s \sqsubseteq_a s'$  :iff there is  $s'' \in \mathcal{S}$  such that  $\pi_a(s) \star \pi_a(s'') = \pi_a(s')$ ;
- $\sqsubseteq := \sqsubseteq_{\text{CM}}$  designate the (global) *state **partial order*** serving as the concrete accessibility relation in the Kripke-semantics for the I-fragment of LliP;  
( $\sqsubseteq$  is partial thanks to **CM** seeing any agent’s input events.)
- $\equiv_a := \sqsubseteq_a \cap (\sqsubseteq_a)^{-1}$  designate the (local) *state equivalence of  $a$* ;

- ${}_M R_{\mathbf{CM}} \subseteq \mathcal{S} \times \mathcal{S}$  designate the **concretely constructed accessibility relation**—short, **concrete accessibility**—for LliP such that for all  $s, s' \in \mathcal{S}$ ,

$$s {}_M R_{\mathbf{CM}} s' \text{ :iff } \begin{array}{l} s' \in \bigcup_{\substack{s \sqsubseteq_{\mathbf{CM}} \tilde{s} \text{ and} \\ M \in \text{cl}_{\mathbf{CM}}^{\tilde{s}}(\emptyset)}} [\tilde{s}]_{\equiv_{\mathbf{CM}}} \\ \text{(iff there is } \tilde{s} \in \mathcal{S} \text{ s.t. } s \sqsubseteq_{\mathbf{CM}} \tilde{s} \text{ and } M \in \text{cl}_{\mathbf{CM}}^{\tilde{s}}(\emptyset) \text{ and } \tilde{s} \equiv_{\mathbf{CM}} s'). \end{array}$$

Note that the data-mining operator  $\text{cl}_a : 2^{\mathcal{M}} \rightarrow 2^{\mathcal{M}}$  is a compact closure operator, which induces a *data-derivation relation*  $\vdash_a \subseteq 2^{\mathcal{M}} \times \mathcal{M}$  such that  $\mathcal{D} \vdash_a M$  :iff  $M \in \text{cl}_a(\mathcal{D})$ , which (1) has the compactness and (2) the cut property, (3) is decidable in deterministic polynomial time in the size of  $\mathcal{D}$  and  $M$ , and (4) induces a Scott information system of information tokens  $M$  [Kra12a].

**Fact 1.**

1.  $\equiv_{\mathbf{CM}} = \text{Id}_{\mathcal{S}}$
2.  $s {}_M R_{\mathbf{CM}} s'$  if and only if  $(s \sqsubseteq s' \text{ and } M \in \text{cl}_{\mathbf{CM}}^{s'}(\emptyset))$
3.  ${}_{\mathbf{CM}} R_{\mathbf{CM}} = \sqsubseteq$

*Proof.* By inspection of definitions.  $\square$

Fact 1.1 is important, because thanks to it the communication medium  $\mathbf{CM}$  can have perfect knowledge, as asserted on Page 18; and Fact 1.3 is, because thanks to it the partial order  $\sqsubseteq$  for the Kripke-semantics of LliP's intuitionistic connectives is absorbed as a mere instance  ${}_{\mathbf{CM}} R_{\mathbf{CM}}$  of the accessibility relation  ${}_M R_{\mathbf{CM}}$  for the Kripke-semantics of LliP's proof modality, as announced on Page 7. Fact 1.2 captures the intuition of the concrete accessibility of LliP. Spelled out, this intuition is that  $\mathbf{CM}$  can access an input history  $s'$  from the current input history  $s$  with respect to a piece of data  $M$  in question if and only if  $s'$  is an extension of  $s$  such that  $M$  is in  $\mathbf{CM}$ 's individual-knowledge base at  $s'$ . A simple example is that  $0 {}_{\mathbf{CM}} R_M \text{succ}_a^M(0)$ , because  $0 \sqsubseteq \text{succ}_a^M(0)$  and  $M \in \text{cl}_{\mathbf{CM}}^{\text{succ}_a^M(0)}(\emptyset)$ . A slightly more complex example is that  $0 {}_{\mathbf{CM}} R_{M'} \text{succ}_b^{(M, M')}(\text{succ}_a^M(0))$ , because  $0 \sqsubseteq \text{succ}_b^{(M, M')}(\text{succ}_a^M(0))$  and  $M' \in \text{cl}_{\mathbf{CM}}^{\text{succ}_b^{(M, M')}(\text{succ}_a^M(0))}(\emptyset)$ .

We need the following auxiliary definition for the proposition following it.

**Definition 4** (Message pre-ordering [Kra12a, Kra13c]).

- $M \sqsubseteq_a^s M'$  :iff if  $M \in \text{cl}_a^s(\emptyset)$  then  $M' \in \text{cl}_a^s(\emptyset)$
- $M \sqsubseteq_a M'$  :iff for all  $s \in \mathcal{S}$ ,  $M \sqsubseteq_a^s M'$

Notice the definitional overloading of the notation  $\sqsubseteq_a$ , i.e., once as  $\sqsubseteq_a \subseteq \mathcal{S} \times \mathcal{S}$  in Definition 3 and once as  $\sqsubseteq_a \subseteq \mathcal{M} \times \mathcal{M}$  in the previous Definition 4.

**Proposition 2** (Concrete accessibility).

Table 2: Satisfaction relation

$(\mathfrak{S}, \mathcal{V}), s \models P$	:iff	$s \in \mathcal{V}(P)$
$(\mathfrak{S}, \mathcal{V}), s \models \phi \vee \phi'$	:iff	$(\mathfrak{S}, \mathcal{V}), s \models \phi$ or $(\mathfrak{S}, \mathcal{V}), s \models \phi'$
$(\mathfrak{S}, \mathcal{V}), s \models \phi \wedge \phi'$	:iff	$(\mathfrak{S}, \mathcal{V}), s \models \phi$ and $(\mathfrak{S}, \mathcal{V}), s \models \phi'$
$(\mathfrak{S}, \mathcal{V}), s \models \neg\phi$	:iff	for all $s' \in \mathcal{S}$ , if $s \sqsubseteq s'$ then not $(\mathfrak{S}, \mathcal{V}), s' \models \phi$
$(\mathfrak{S}, \mathcal{V}), s \models \phi \rightarrow \phi'$	:iff	for all $s' \in \mathcal{S}$ , if $s \sqsubseteq s'$ then $(\mathfrak{S}, \mathcal{V}), s' \models \phi$ or $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$
$(\mathfrak{S}, \mathcal{V}), s \models M \pm_{\text{CM}} \phi$	:iff	for all $s' \in \mathcal{S}$ , if $s \mathrel{M\mathcal{R}_{\text{CM}}} s'$ then $(\mathfrak{S}, \mathcal{V}), s' \models \phi$

1. If  $s \mathrel{M\mathcal{R}_{\text{CM}}} s'$  then  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$  (epistemic image)
2. If  $M \in \text{cl}_{\text{CM}}^s(\emptyset)$  then  $s \mathrel{M\mathcal{R}_{\text{CM}}} s$  (conditional reflexivity)
3. there is  $s' \in \mathcal{S}$  such that  $s \mathrel{M\mathcal{R}_{\text{CM}}} s'$  (seriality)
4.  $M\mathcal{R}_{\text{CM}} \subseteq \text{CM}\mathcal{R}_{\text{CM}} = \sqsubseteq$  (MIAR-inclusion)
5.  $(\text{CM}\mathcal{R}_{\text{CM}} \circ M\mathcal{R}_{\text{CM}}) \subseteq M\mathcal{R}_{\text{CM}}$  (special transitivity)
6. If  $M \sqsubseteq_{\text{CM}} M'$  then  $M\mathcal{R}_{\text{CM}} \subseteq M'\mathcal{R}_{\text{CM}}$  (proof monotonicity)

*Proof.* For 1, inspect Fact 1.2. For 2, inspect Fact 1.2 and 1.3 and the definition of  $\sqsubseteq$  (to see that  $\sqsubseteq$  is reflexive). For 3, inspect Fact 1.2 and let  $s \in \mathcal{S}$ . Then choose  $s' = \text{succ}_{\text{CM}}^M(s) \in \mathcal{S}$ , which implies that  $s \sqsubseteq s'$  and  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$ . For 4, inspect Fact 1.2 and 1.3 and the definitional fact that  $\text{CM} \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$ . For 5, let  $s, s' \in \mathcal{S}$  and suppose that  $s (\text{CM}\mathcal{R}_{\text{CM}} \circ M\mathcal{R}_{\text{CM}}) s'$ . That is, there is  $s'' \in \mathcal{S}$  such that  $s \mathrel{\text{CM}\mathcal{R}_{\text{CM}}} s''$  and  $s'' \mathrel{M\mathcal{R}_{\text{CM}}} s'$ . Hence,  $s \sqsubseteq s''$  and  $\text{CM} \in \text{cl}_{\text{CM}}^{s''}(\emptyset)$  as well as  $s'' \sqsubseteq s'$  and  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$ , by Fact 1.2. Hence  $s \sqsubseteq s'$  by the transitivity of  $\sqsubseteq$ . Hence  $s \mathrel{M\mathcal{R}_{\text{CM}}} s'$  by Fact 1.2. For 6, let  $M, M' \in \mathcal{M}$  and suppose that  $M \sqsubseteq_{\text{CM}} M'$ . Further, let  $s, s' \in \mathcal{S}$  and suppose that  $s \mathrel{M\mathcal{R}_{\text{CM}}} s'$ . Hence  $M \sqsubseteq_{\text{CM}}^{s'} M'$ , and also  $s \sqsubseteq s'$  and  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$  by Fact 1.2. Hence  $M' \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$ . Hence  $s \mathrel{M'\mathcal{R}_{\text{CM}}} s'$  by Fact 1.2.  $\square$

Note that “MIAR” stands for “modal-intuitionistic-accessibility-relation.”

### 2.2.2 Abstractly

**Definition 5** (Kripke-model). We define the *satisfaction relation*  $\models$  for LliP in Table 2, where

- $\mathcal{V} : \mathcal{P} \rightarrow 2^{\mathcal{S}}$  designates a usual *valuation function*, yet
  - *partially predefined* such that for all  $a \in \mathcal{A}$  and  $M \in \mathcal{M}$ ,

$$\mathcal{V}(a \mathrel{K} M) := \{ s \in \mathcal{S} \mid M \in \text{cl}_a^s(\emptyset) \};$$

(If agents are Turing-machines then  $a$  knowing  $M$  can be understood as  $a$  being able to parse  $M$  on its tape.)

– *constrained* such that for all  $s, s' \in \mathcal{S}$ ,

$$\text{if } s \in \mathcal{V}(P) \text{ and } s \sqsubseteq s' \text{ then } s' \in \mathcal{V}(P);$$

(following Kripke’s semantics for IL)

- $\mathfrak{S} := (\mathcal{S}, \sqsubseteq, \{ {}_M\mathcal{R}_{\text{CM}} \}_{M \in \mathcal{M}})$  designates an intuitionistic modal *frame* for LliP with a usual partial order  $\sqsubseteq \subseteq \mathcal{S} \times \mathcal{S}$  for the intuitionistic part as well as an **abstractly constrained accessibility relation**—short, **abstract accessibility**— ${}_M\mathcal{R}_{\text{CM}} \subseteq \mathcal{S} \times \mathcal{S}$  for LliP such that—the *semantic interface*:

- If  $s {}_M\mathcal{R}_{\text{CM}} s'$  then  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$
- If  $M \in \text{cl}_{\text{CM}}^s(\emptyset)$  then  $s {}_M\mathcal{R}_{\text{CM}} s$
- there is  $s' \in \mathcal{S}$  such that  $s {}_M\mathcal{R}_{\text{CM}} s'$
- ${}_M\mathcal{R}_{\text{CM}} \subseteq {}_{\text{CM}}\mathcal{R}_{\text{CM}} = \sqsubseteq$
- $({}_{\text{CM}}\mathcal{R}_{\text{CM}} \circ {}_M\mathcal{R}_{\text{CM}}) \subseteq {}_M\mathcal{R}_{\text{CM}}$
- If  $M \sqsubseteq_{\text{CM}} M'$  then  ${}_M\mathcal{R}_{\text{CM}} \subseteq {}_{M'}\mathcal{R}_{\text{CM}}$

- $(\mathfrak{S}, \mathcal{V})$  designates an intuitionistic modal *model* for LliP.

Looking back, we recognise that Proposition 2 actually establishes the important fact that our concrete accessibility  ${}_M\mathcal{R}_{\text{CM}}$  in Definition 3 realises all the properties stipulated by our abstract accessibility  ${}_M\mathcal{R}_{\text{CM}}$  in Definition 5; we say that

$${}_M\mathcal{R}_{\text{CM}} \text{ exemplifies (or realises) } {}_M\mathcal{R}_{\text{CM}}.$$

Further, observe that LliP (like LiP) has a Herbrand-style semantics, i.e., logical constants (agent names) and functional symbols (pairing) are self-interpreted rather than interpreted in terms of (other, semantic) constants and functions. This simplifying design choice spares our framework from the additional complexity that would arise from term-variable assignments [BG07], which in turn keeps our models propositionally modal. Our choice is admissible because our individuals (messages) are finite. (Infinitely long “messages” are non-messages; they can never be completely received, e.g., transmitting irrational numbers as such is impossible.)

**Definition 6** (Truth & Validity [BvB07]).

- The formula  $\phi \in \mathcal{L}$  is *true* (or *satisfied*) in the model  $(\mathfrak{S}, \mathcal{V})$  at the state  $s \in \mathcal{S}$  :iff  $(\mathfrak{S}, \mathcal{V}), s \models \phi$ .
- The formula  $\phi$  is *satisfiable* in the model  $(\mathfrak{S}, \mathcal{V})$  :iff there is  $s \in \mathcal{S}$  such that  $(\mathfrak{S}, \mathcal{V}), s \models \phi$ .
- The formula  $\phi$  is *globally true* (or *globally satisfied*) in the model  $(\mathfrak{S}, \mathcal{V})$ , written  $(\mathfrak{S}, \mathcal{V}) \models \phi$ , :iff for all  $s \in \mathcal{S}$ ,  $(\mathfrak{S}, \mathcal{V}), s \models \phi$ .

- The formula  $\phi$  is *satisfiable* :iff there is a model  $(\mathfrak{S}, \mathcal{V})$  and a state  $s \in \mathcal{S}$  such that  $(\mathfrak{S}, \mathcal{V}), s \models \phi$ .
- The formula  $\phi$  is *valid*, written  $\models \phi$ , :iff for all models  $(\mathfrak{S}, \mathcal{V})$ ,  $(\mathfrak{S}, \mathcal{V}) \models \phi$ .

The following lemma is a *passage obligé* in the construction of a Kripke-semantics for any intuitionistic logic, modal or not, and thus also for ours.

**Lemma 1** (Monotonicity Lemma). *For all LliP-models  $(\mathfrak{S}, \mathcal{V})$ ,  $s, s' \in \mathcal{S}$ , and  $\phi \in \mathcal{L}$ , if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi$ .*

*Proof.* Let  $(\mathfrak{S}, \mathcal{V})$  designate an arbitrary LliP-model and let  $s, s' \in \mathcal{S}$ . Then let us proceed by induction on the structure of  $\phi \in \mathcal{L}$  :

- Base case ( $\phi := P$  for an arbitrary  $P \in \mathcal{P} \subseteq \mathcal{L}$ ). Suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models P$ . Thus  $s \in \mathcal{V}(P)$ , by definition. Hence  $s' \in \mathcal{V}(P)$ , by the definitional constraint on  $\mathcal{V}$ . Thus  $(\mathfrak{S}, \mathcal{V}), s' \models P$ , by definition.
- Inductive steps:
  - $\phi := \phi' \vee \phi''$  for arbitrary  $\phi', \phi'' \in \mathcal{L}$ . For the sake of the induction, suppose that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$  and that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi''$ . Further suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi' \vee \phi''$ . Thus  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  or  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$ , by definition. Let us proceed by disjunctive case analysis:
    - \* Suppose that  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$ . Hence  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$ , by induction hypothesis. Hence  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$  or  $(\mathfrak{S}, \mathcal{V}), s' \models \phi''$ , by meta-level (classical) propositional logic. Thus  $(\mathfrak{S}, \mathcal{V}), s' \models \phi' \vee \phi''$ , by definition.
    - \* Suppose that  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$ , and proceed symmetrically to the previous case.
  - $\phi := \phi' \wedge \phi''$  for arbitrary  $\phi', \phi'' \in \mathcal{L}$ . For the sake of the induction, suppose that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$  and that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi''$ . Further suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi' \wedge \phi''$ . Thus  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$ , by definition. Hence  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$  and  $(\mathfrak{S}, \mathcal{V}), s' \models \phi''$ , by the induction hypotheses. Thus  $(\mathfrak{S}, \mathcal{V}), s' \models \phi' \wedge \phi''$ , by definition.
  - $\phi := \neg\phi'$  for an arbitrary  $\phi' \in \mathcal{L}$ . For the sake of the induction, suppose that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$ . Further suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \neg\phi'$ . Thus for all  $s'' \in \mathcal{S}$ , if  $s \sqsubseteq s''$  then not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$ , by definition. Now, let  $s'' \in \mathcal{S}$  and further suppose that  $s' \sqsubseteq s''$ . Hence  $s \sqsubseteq s''$ , by the transitivity of  $\sqsubseteq$ . Hence not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$ . Hence for all  $s'' \in \mathcal{S}$ , if  $s' \sqsubseteq s''$  then not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$ . Thus  $(\mathfrak{S}, \mathcal{V}), s' \models \neg\phi'$ , by definition. (Observe that the induction hypothesis turns out to be irrelevant for this case.)

- $\phi := \phi' \rightarrow \phi''$  for arbitrary  $\phi', \phi'' \in \mathcal{L}$ . For the sake of the induction, suppose that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$  and that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi''$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi''$ . Further suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi' \rightarrow \phi''$ . Thus for all  $s'' \in \mathcal{S}$ , if  $s \sqsubseteq s''$  then (not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$  or  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi''$ ), by definition. Now, let  $s'' \in \mathcal{S}$  and further suppose that  $s' \sqsubseteq s''$ . Hence  $s \sqsubseteq s''$ , by the transitivity of  $\sqsubseteq$ . Hence, not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$  or  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi''$ . Hence for all  $s'' \in \mathcal{S}$ , if  $s' \sqsubseteq s''$  then (not  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$  or  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi''$ ). Thus  $(\mathfrak{S}, \mathcal{V}), s' \models \phi' \rightarrow \phi''$ , by definition. (Observe that the induction hypotheses turn out to be irrelevant for this case.)
- $\phi := M \pm_{\text{CM}} \phi'$  for an arbitrary  $\phi' \in \mathcal{L}$ . For the sake of the induction, suppose that if  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models \phi'$  then  $(\mathfrak{S}, \mathcal{V}), s' \models \phi'$ . Further suppose that  $s \sqsubseteq s'$  and  $(\mathfrak{S}, \mathcal{V}), s \models M \pm_{\text{CM}} \phi'$ . Thus on the one hand,  $s \text{ CMR}_{\text{CM}} s'$ , by MIAR-inclusion, and also, on the other hand, for all  $s'' \in \mathcal{S}$ , if  $s \text{ MR}_{\text{CM}} s''$  then  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$ , by definition. Now, let  $s'' \in \mathcal{S}$  and further suppose that  $s' \text{ MR}_{\text{CM}} s''$ . Hence  $s \text{ MR}_{\text{CM}} s''$ , by special transitivity. Hence  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi'$ . (Observe that the induction hypothesis turns out to be irrelevant for this case.)

□

Observe that the induction hypothesis in the proof turns out to be irrelevant for all negative connectives and the modality, which are made to conserve the monotonicity of atomic propositions (cf. Page 4).

**Proposition 3** (Concrete LliP-models). *Let  $\mathfrak{M}$  designate an arbitrary concrete LliP-model, i.e., a model with ingredients like in Definition 3, and let  $\phi \in \mathcal{L}$ .*

*Then,*

$$\mathfrak{M}, 0 \models \phi \text{ if and only if } \mathfrak{M} \models \phi.$$

*Proof.* The only-if direction follows from the definition of global satisfaction (cf. Definition 6). For the if-direction, consider that the concrete state space  $\mathcal{S} = \{ s \in \mathcal{S} \mid 0 \sqsubseteq s \}$  and apply the antecedent Monotonicity Lemma. □

**Proposition 4** (Admissibility of LliP-specific axioms and rules).

1.  $\models a \text{ k } a$
2.  $\models (a \text{ k } M \wedge a \text{ k } M') \leftrightarrow a \text{ k } (M, M')$
3.  $\models M \pm_{\text{CM}} \text{CM k } M$
4.  $\models (M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi')$
5.  $\models (M \pm_{\text{CM}} \phi) \rightarrow (\text{CM k } M \rightarrow \phi)$
6.  $\models (M \pm_{\text{CM}} \phi) \rightarrow (M \mp_{\text{CM}} \phi)$
7.  $\models \phi \rightarrow M \pm_{\text{CM}} \phi$



8. If  $\models \phi$  then  $\models M \pm_{\text{CM}} \phi$
9. If  $\models \text{CM} k M \rightarrow \text{CM} k M'$  then  $\models (M' \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi$ .

*Proof.* 1 and 2 are immediate; 4 and 8 hold by the fact that LliP has a standard Kripke-semantics; 3 follows directly from the epistemic-image property of  ${}_M\mathcal{R}_{\text{CM}}$ , 5 from the conditional reflexivity of  ${}_M\mathcal{R}_{\text{CM}}$ , and 9 from the proof-monotonicity property of  ${}_M\mathcal{R}_{\text{CM}}$ . 6 follows from the seriality of  ${}_M\mathcal{R}_{\text{CM}}$  and the MIAR-inclusion and the epistemic-image property of  ${}_M\mathcal{R}_{\text{CM}}$  as follows: Let  $(\mathfrak{S}, \mathcal{V})$  designate an arbitrary LliP-model and let  $s \in \mathcal{S}$ . Further let  $s' \in \mathcal{S}$  and suppose that  $s \sqsubseteq s'$ . Now suppose that  $(\mathfrak{S}, \mathcal{V}), s' \models M \pm_{\text{CM}} \phi$ . Further let  $s'' \in \mathcal{S}$  and suppose that  $s' \sqsubseteq s''$ . Hence  $(\mathfrak{S}, \mathcal{V}), s'' \models M \pm_{\text{CM}} \phi$  by the Monotonicity Lemma. That is, for all  $s''' \in \mathcal{S}$ , if  $s'' {}_M\mathcal{R}_{\text{CM}} s'''$  then  $(\mathfrak{S}, \mathcal{V}), s''' \models \phi$ . But by the seriality of  ${}_M\mathcal{R}_{\text{CM}}$ , there is indeed an  $s''' \in \mathcal{S}$  such that  $s'' {}_M\mathcal{R}_{\text{CM}} s'''$ . Hence,  $(\mathfrak{S}, \mathcal{V}), s''' \models \phi$ , and also  $s'' \sqsubseteq s'''$  by the MIAR-inclusion property, and yet also  $M \in \text{cl}_{\text{CM}}^{s'''}(\emptyset)$  by the epistemic-image property. Thus  $(\mathfrak{S}, \mathcal{V}), s''' \models \text{CM} k M \wedge \phi$ . Hence  $(\mathfrak{S}, \mathcal{V}), s' \models \neg\neg(\text{CM} k M \wedge \phi)$  and thus  $(\mathfrak{S}, \mathcal{V}), s \models (M \pm_{\text{CM}} \phi) \rightarrow \neg\neg(\text{CM} k M \wedge \phi)$ . Finally, 7 follows from the MIAR-inclusion property of  ${}_M\mathcal{R}_{\text{CM}}$  and the Monotonicity Lemma (which in turn holds thanks to the special transitivity and the MIAR-inclusion property of  ${}_M\mathcal{R}_{\text{CM}}$ ) as follows: Let  $(\mathfrak{S}, \mathcal{V})$  designate an arbitrary LliP-model and let  $s \in \mathcal{S}$ . Further let  $s' \in \mathcal{S}$  and suppose that  $s \sqsubseteq s'$ . Now suppose that  $(\mathfrak{S}, \mathcal{V}), s' \models \phi$ . Additionally, let  $s'' \in \mathcal{S}$  and suppose that  $s' {}_M\mathcal{R}_{\text{CM}} s''$ . Hence  $s' \sqsubseteq s''$  by MIAR-inclusion. Hence  $(\mathfrak{S}, \mathcal{V}), s'' \models \phi$  by the Monotonicity Lemma. Thus,  $(\mathfrak{S}, \mathcal{V}), s' \models M \pm_{\text{CM}} \phi$ , and then  $(\mathfrak{S}, \mathcal{V}), s \models \phi \rightarrow M \pm_{\text{CM}} \phi$ .  $\square$

**Theorem 3** (Axiomatic adequacy).  $\vdash_{\text{LliP}}$  is adequate for  $\models$ , i.e.,:

1. if  $\vdash_{\text{LliP}} \phi$  then  $\models \phi$  (axiomatic soundness)
2. if  $\models \phi$  then  $\vdash_{\text{LliP}} \phi$  (semantic completeness).

*Proof.* Both parts can be proved with standard means: axiomatic soundness follows from the admissibility of the axioms and rules (cf. Proposition 4) as usual, and semantic completeness follows by means of a construction of canonical models that is appropriate for intuitionistic normal modal logic as follows.

Let

- $\mathcal{W}$  designate the set of all prime LliP-consistent sets<sup>5</sup>
- $w \sqsubseteq w' : \text{iff } w \subseteq w'$
- for all  $w, w' \in \mathcal{W}$ ,  $w {}_M\mathcal{C}_{\text{CM}} w' : \text{iff } \{ \phi \in \mathcal{L} \mid M \pm_{\text{CM}} \phi \in w \} \subseteq w'$

<sup>5\*</sup> A set  $W$  of LliP-formulas is prime LliP-consistent :iff  $W$  is LliP-consistent and  $W$  is prime. A set  $W$  of LliP-formulas is LliP-consistent :iff  $W$  is not LliP-inconsistent. A set  $W$  of LliP-formulas is LliP-inconsistent :iff there is a finite  $W' \subseteq W$  such that  $((\bigwedge W') \rightarrow \perp) \in \text{LliP}$ . A set  $W$  of LliP-formulas is prime :iff first,  $W$  is deductively closed, that is, there is a finite  $W' \subseteq W$  such that for all  $\phi \in \mathcal{L}$ , if  $((\bigwedge W') \rightarrow \phi) \in \text{LliP}$  then  $\phi \in W$ , and second,  $W$  has the disjunction property, that is, for all  $\phi, \phi' \in \mathcal{L}$ , if  $\phi \vee \phi' \in W$  then  $\phi \in W$  or  $\phi' \in W$ . Similar to a classical Lindenbaum construction (extending consistent sets to *maximal* consistent sets) any LliP-consistent set can be extended to a *prime* LliP-consistent set.

- for all  $w \in \mathcal{W}$ ,  $w \in \mathcal{V}_C(P)$  :iff  $P \in w$ .

Then  $\mathfrak{M}_C := (\mathcal{W}, \sqsubseteq, \{ {}_M C_{\mathbf{CM}} \}_{M \in \mathcal{M}}, \mathcal{V}_C)$  designates the *canonical model* for LliP.

Following standard practice common to all intuitionistic normal modal logics, the following useful property of  $\mathfrak{M}_C$ , the so-called *Truth Lemma*,

$$\text{for all } \phi \in \mathcal{L} \text{ and } w \in \mathcal{W}, \phi \in w \text{ if and only if } \mathfrak{M}_C, w \models \phi$$

can be proved by induction on the structure of  $\phi$ . With this lemma, it can then be proved that for all  $\phi \in \mathcal{L}$ , if  $\not\models_{\text{LliP}} \phi$  then  $\not\models \phi$ . Let  $\phi \in \mathcal{L}$ , and suppose that  $\not\models_{\text{LliP}} \phi$ . Thus,  $\{\neg\phi\}$  is LliP-consistent, and can be extended to a prime LliP-consistent set  $w$ , i.e.,  $\neg\phi \in w \in \mathcal{W}$ . Hence  $\mathfrak{M}_C, w \models \neg\phi$ , by the Truth Lemma. Thus:  $\mathfrak{M}_C, w \not\models \phi$ ,  $\mathfrak{M}_C \not\models \phi$ , and  $\not\models \phi$ . That is,  $\mathfrak{M}_C$  is a *universal* (for all  $\phi \in \mathcal{L}$ ) *counter-model* (if  $\phi$  is a non-theorem then  $\mathfrak{M}_C$  falsifies  $\phi$ ).

The only proof obligation specific to the semantic-completeness proof for LliP is to prove that  $\mathfrak{M}_C$  is also an *LliP-model*. So let us instantiate our data-mining operator  $\text{cl}_a$  (cf. Page 19) on  $\mathcal{W}$  by letting for all  $w \in \mathcal{W}$

$$\text{msgs}_a(w) := \{ M \mid a \mathbf{k} M \in w \},$$

and let us prove that:

1. If  $w {}_M C_{\mathbf{CM}} w'$  then  $M \in \text{cl}_{\mathbf{CM}}^{w'}(\emptyset)$
2. If  $M \in \text{cl}_{\mathbf{CM}}^w(\emptyset)$  then  $w {}_M C_{\mathbf{CM}} w$
3. there is  $w' \in \mathcal{W}$  such that  $w {}_M C_{\mathbf{CM}} w'$
4.  ${}_M C_{\mathbf{CM}} \subseteq {}_{\mathbf{CM}} C_{\mathbf{CM}} = \sqsubseteq$
5.  $({}_{\mathbf{CM}} C_{\mathbf{CM}} \circ {}_M C_{\mathbf{CM}}) \subseteq {}_M C_{\mathbf{CM}}$
6. If  $M \sqsubseteq_{\mathbf{CM}} M'$  then  ${}_M C_{\mathbf{CM}} \subseteq {}_{M'} C_{\mathbf{CM}}$

For (1), let  $w, w' \in \mathcal{W}$  and suppose that  $w {}_M C_{\mathbf{CM}} w'$ . That is, for all  $\phi \in \mathcal{L}$ , if  $M \pm_{\mathbf{CM}} \phi \in w$  then  $\phi \in w'$ . Since  $w$  is deductively closed,

$$M \pm_{\mathbf{CM}} {}_{\mathbf{CM}} \mathbf{k} M \in w \quad (\text{self-knowledge}).$$

Hence  ${}_{\mathbf{CM}} \mathbf{k} M \in w'$ . Thus  $M \in \text{cl}_{\mathbf{CM}}^{w'}(\emptyset)$  by the definition of  $\text{cl}_{\mathbf{CM}}^{w'}$ .

For (2), let  $w \in \mathcal{W}$  and suppose that  $M \in \text{cl}_{\mathbf{CM}}^w(\emptyset)$ . Hence  ${}_{\mathbf{CM}} \mathbf{k} M \in w$  due to the deductive closure of  $w$ . Further suppose that  $M \pm_{\mathbf{CM}} \phi \in w$ . Since  $w$  is deductively closed,

$$(M \pm_{\mathbf{CM}} \phi) \rightarrow ({}_{\mathbf{CM}} \mathbf{k} M \rightarrow \phi) \in w \quad (\text{ET}).$$

Hence,  ${}_{\mathbf{CM}} \mathbf{k} M \rightarrow \phi \in w$ , and  $\phi \in w$ , by consecutive *modus ponens*.

For (3), let  $w \in \mathcal{W}$  and  $\phi \in \mathcal{L}$ , and suppose that  $M \pm_{\mathbf{CM}} \phi \in w$ . Since  $w$  is deductively closed,

$$(M \pm_{\mathbf{CM}} \phi) \rightarrow M \mp_{\mathbf{CM}} \phi \in w \quad (\text{ID}).$$

Hence,  $M \mp_{\text{CM}} \phi \in w$  by *modus ponens*. That is,  $\neg\neg(\text{CM } k M \wedge \phi) \in w$  by definition. Since  $w$  is deductively closed,  $\neg\neg(\text{CM } k M \wedge \phi) \rightarrow \neg\neg\phi \in w$ . Hence  $\neg\neg\phi \in w$  by *modus ponens*. Hence  $\mathfrak{M}_{\text{C}}, w \models \neg\neg\phi$  by the Truth Lemma. Hence for all  $w' \in \mathcal{W}$ , if  $w \sqsubseteq w'$  then there is  $w'' \in \mathcal{W}$  such that  $w' \sqsubseteq w''$  and  $\mathfrak{M}_{\text{C}}, w'' \models \phi$  by definition. Hence  $\phi \in w''$  by the Truth Lemma.

For (4), let us first prove that  $_{\text{CM}}C_{\text{CM}} = \sqsubseteq$ . So let  $w, w' \in \mathcal{W}$  and suppose that  $w \text{ } _{\text{CM}}C_{\text{CM}} w'$ . That is, for all  $\phi \in \mathcal{L}$ , if  $\text{CM } \pm_{\text{CM}} \phi \in w$  then  $\phi \in w'$ . Further let  $\phi \in \mathcal{L}$  and suppose that  $\phi \in w$ . Hence if  $\text{CM } \pm_{\text{CM}} \phi \in w$  then  $\phi \in w'$ . Since  $w$  is deductively closed,

$$(\text{CM } \pm_{\text{CM}} \phi) \leftrightarrow \phi \in w \quad (\text{TMM})$$

Hence  $\text{CM } \pm_{\text{CM}} \phi \in w$  by *LliP-modus ponens*. Hence  $\phi \in w'$  by meta-level *modus ponens*. Thus  $w \subseteq w'$ , and then  $w \sqsubseteq w'$ . Conversely, suppose that  $w \sqsubseteq w'$ . That is,  $w \subseteq w'$ . Further let  $\phi \in \mathcal{L}$  and suppose that  $\text{CM } \pm_{\text{CM}} \phi \in w$ . Hence  $\text{CM } \pm_{\text{CM}} \phi \in w'$ . Since  $w'$  is deductively closed,

$$(\text{CM } \pm_{\text{CM}} \phi) \leftrightarrow \phi \in w' \quad (\text{TMM})$$

Hence  $\phi \in w'$  by *LliP-modus ponens*. Second, let us prove that  ${}_M C_{\text{CM}} \subseteq {}_{\text{CM}}C_{\text{CM}}$ . So let  $w, w' \in \mathcal{W}$  and suppose that  $w {}_M C_{\text{CM}} w'$ . That is, for all  $\phi \in \mathcal{L}$ , if  $M \pm_{\text{CM}} \phi \in w$  then  $\phi \in w'$ . Further let  $\phi \in \mathcal{L}$  and suppose that  $\text{CM } \pm_{\text{CM}} \phi \in w$ . Since  $w$  is deductively closed,

$$(\text{CM } \pm_{\text{CM}} \phi) \leftrightarrow \phi \in w \quad (\text{TMM})$$

Hence  $\phi \in w$  by *LliP-modus ponens*. Since  $w$  is deductively closed,

$$\phi \rightarrow M \pm_{\text{CM}} \phi \in w \quad (\text{MM})$$

Hence  $M \pm_{\text{CM}} \phi \in w$  by *LliP-modus ponens*. Hence  $\phi \in w'$  by meta-level *modus ponens*.

For (5), let  $w, w' \in \mathcal{W}$  and suppose that  $w ({}_{\text{CM}}C_{\text{CM}} \circ {}_M C_{\text{CM}}) w'$ . That is, there is  $w'' \in \mathcal{W}$  such that  $w {}_{\text{CM}}C_{\text{CM}} w''$  and  $w'' {}_M C_{\text{CM}} w'$ . Thus, (for all  $\phi \in \mathcal{L}$ , if  $\text{CM } \pm_{\text{CM}} \phi \in w$  then  $\phi \in w''$ ) and (for all  $\phi \in \mathcal{L}$ , if  $M \pm_{\text{CM}} \phi \in w''$  then  $\phi \in w'$ ). Further let  $\phi \in \mathcal{L}$  and suppose that  $M \pm_{\text{CM}} \phi \in w$ . Since  $w$  is deductively closed,

$$(\text{CM } \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \leftrightarrow M \pm_{\text{CM}} \phi \in w \quad (\text{TMM})$$

Hence  $(\text{CM } \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \in w$ . Hence  $M \pm_{\text{CM}} \phi \in w''$  by the first hypothesis. Hence  $\phi \in w'$  by the second hypothesis. Thus  $w {}_M C_{\text{CM}} w'$ .

For (6), suppose that  $M \sqsubseteq_{\text{CM}} M'$ . That is, for all  $w \in \mathcal{W}$ , if  $M \in \text{cl}_{\text{CM}}^w(\emptyset)$  then  $M' \in \text{cl}_{\text{CM}}^w(\emptyset)$ . Hence for all  $w \in \mathcal{W}$ , if  $\text{CM } k M \in w$  then  $\text{CM } k M' \in w$  due to the deductive closure of  $w$ , which contains all the term axioms corresponding to the defining clauses of  $\text{cl}_{\text{CM}}^w$ . Hence for all  $w \in \mathcal{W}$ , if  $\mathfrak{M}_{\text{C}}, w \models \text{CM } k M$  then  $\mathfrak{M}_{\text{C}}, w \models \text{CM } k M'$ , by the Truth Lemma. Hence also, for all  $w \in \mathcal{W}$ ,  $\mathfrak{M}_{\text{C}}, w \models \text{CM } k M \rightarrow \text{CM } k M'$  by the definition of  $\sqsubseteq$ . Hence for all  $w \in \mathcal{W}$ ,  $\text{CM } k M \rightarrow \text{CM } k M' \in w$  by the Truth Lemma. Hence the following intermediate result, called IR,

$$\text{for all } w \in \mathcal{W} \text{ and } \phi \in \mathcal{L}, (M' \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi \in w,$$

by EA. Now, let  $w, w' \in \mathcal{W}$  and suppose that  $w \mathrel{MC_{\mathcal{M}}} w'$ . That is, for all  $\phi \in \mathcal{L}$ , if  $M \pm_{\mathcal{M}} \phi \in w$  then  $\phi \in w'$ . Hence, for all  $\phi \in \mathcal{L}$ , if  $M' \pm_{\mathcal{M}} \phi \in w$  then  $\phi \in w'$  by IR. Hence  $w \mathrel{MC_{\mathcal{M}}} w'$  by definition.  $\square$

**Theorem 4** (Finite-model property). *For any LliP-model  $\mathfrak{M}$ , if  $\mathfrak{M}, s \models \phi$  then there is a finite LliP-model  $\mathfrak{M}_{\text{fin}}$  such that  $\mathfrak{M}_{\text{fin}}, s \models \phi$ .*

*Proof.* By the fact that the *minimal filtration* [GO07]

$$\mathfrak{M}_{\text{ft}}^{\min, \Gamma} := (\mathcal{S}/\sim_{\Gamma}, \sqsubseteq^{\min, \Gamma}, \{M\mathcal{R}_{\mathcal{M}}^{\min, \Gamma}\}_{M \in \mathcal{M}}, \mathcal{V}_{\Gamma})$$

of any LliP-model  $\mathfrak{M} := (\mathcal{S}, \sqsubseteq, \{M\mathcal{R}_{\mathcal{M}}\}_{M \in \mathcal{M}}, \mathcal{V})$  through a finite  $\Gamma \subseteq \mathcal{L}$  is a finite LliP-model such that for all  $\gamma \in \Gamma$ ,  $\mathfrak{M}, s \models \gamma$  if and only if  $\mathfrak{M}_{\text{ft}}^{\min, \Gamma}, [s]_{\sim_{\Gamma}} \models \gamma$ . Following [GO07] for our setting, we define

$$\begin{aligned} \sim_{\Gamma} &:= \{ (s, s') \in \mathcal{S} \times \mathcal{S} \mid \text{for all } \gamma \in \Gamma, \mathfrak{M}, s \models \gamma \text{ iff } \mathfrak{M}, s' \models \gamma \} \\ \sqsubseteq^{\min, \Gamma} &:= \{ ([s]_{\sim_{\Gamma}}, [s']_{\sim_{\Gamma}}) \mid (s, s') \in \sqsubseteq \} \\ M\mathcal{R}_{\mathcal{M}}^{\min, \Gamma} &:= \{ ([s]_{\sim_{\Gamma}}, [s']_{\sim_{\Gamma}}) \mid (s, s') \in M\mathcal{R}_{\mathcal{M}} \} \\ \mathcal{V}_{\Gamma}(P) &:= \{ [s]_{\sim_{\Gamma}} \mid s \in \mathcal{V}(P) \}. \end{aligned}$$

We further fix  $M \in \text{cl}_{\mathcal{M}}^{[s]_{\sim_{\Gamma}}}(\emptyset)$  :iff  $[s]_{\sim_{\Gamma}} \in \mathcal{V}_{\Gamma}(\text{CMk}M)$ , and choose  $\Gamma$  to be the (finite) sub-formula closure of  $\phi$ . Hence, we are left to prove that  $\mathfrak{M}_{\text{ft}}^{\min, \Gamma}$  is indeed an LliP-model, which means that we are left to prove that  $\sqsubseteq^{\min, \Gamma}$  and  $M\mathcal{R}_{\mathcal{M}}^{\min, \Gamma}$  have all the properties stipulated by the semantic interface of LliP; this is straightforward and therefore relegated to Appendix A.2.  $\square$

**Corollary 7** (Algorithmic decidability). *LliP is algorithmically decidable.*

*Proof.* In order to algorithmically decide whether or not  $\phi \in \text{LliP}$  (that is,  $\vdash_{\text{LliP}} \phi$ ) for some  $\phi \in \mathcal{L}$  (and the current choice of  $\mathcal{M}$ ), axiomatic adequacy allows us to check whether or not  $\neg\phi$  is locally satisfiable (That is, whether or not  $\mathfrak{M}, s \models \neg\phi$  for some LliP-model  $\mathfrak{M}$  and state  $s$ ). Also,  $M \in \text{cl}_{\mathcal{M}}^s(\emptyset)$  on the currently chosen message language  $\mathcal{M}$  is obviously decidable; for other, more complex message languages including cryptographic messages, see for example [TGD10] and [BRS10]). But then, the finite-model property of LliP allows us to enumerate all finite LliP-models  $\mathfrak{M}_{\text{fin}}$  up to a size of at most 2 to the power of the size  $n$  of the sub-formula closure of  $\neg\phi$  and to check whether or not  $\mathfrak{M}_{\text{fin}}, s \models \neg\phi$ . (First, there are at most  $2^n$  equivalence classes for  $n$  formulas. Second, checking intuitionistic negation, which is checking classical negation within the up-set of the state  $s$  with respect to  $\sqsubseteq$ , within a finite model is also a finite task.)  $\square$

Note that the algorithmic complexity of LliP will depend on the specific choice of  $\mathcal{M}$  and the correspondingly chosen term axioms.

### 3 Conclusion

We have produced LliP from LiP with as main contributions those described in Section 1.2. In future work, we shall work out dynamic and first-order extensions of LliP. As roughly related work, we have already mentioned [AI07] (cf. Page 2, 5, 9, and 13) and can further mention [PP13] and [SB13]. In [PP13], a fragment of an intuitionistic version of the minimal Justification Logic [Art08] (mJL) is introduced in the context of an ambitious Curry-Howard isomorphism for modular programming. A similar appreciation can be made of [SB13], which introduced an intuitionistic fragment of the Logic of (non-interactive) Proofs (extending mJL) [AI07]. The main contribution of [PP13] as well as [SB13] seems to be a programming calculus for an axiomatically defined intuitionistic modal logic rather than logic itself, whereas ours is an intuitionistic modal logic with an axiomatics and a set-theoretically constructive semantics.

**Acknowledgements** I thank Olga Grinchtein for spotting a few typos.

### References

- [AI07] S. Artemov and R. Iemhoff. The basic intuitionistic logic of proofs. *The Journal of Symbolic Logic*, 72(2), 2007.
- [And08] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, second edition, 2008.
- [Art08] S. Artemov. The logic of justifications. *The Review of Symbolic Logic*, 1(4), 2008.
- [AtC07] C. Areces and B. ten Cate. *Handbook of Modal Logic*, chapter Hybrid Logics. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [BG07] T. Braüner and S. Ghilardi. *Handbook of Modal Logic*, chapter First-Order Modal Logic. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [BRS10] A. Baskar, R. Ramanujam, and S.P. Suresh. A DEXPTIME-complete Dolev-Yao theory with distributive encryption. In *Proceedings of MFCS*, volume 6281 of *LNCS*. Springer, 2010.
- [BvB07] P. Blackburn and J. van Benthem. *Handbook of Modal Logic*, chapter Modal Logic: A Semantic Perspective. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [BvBW07] P. Blackburn, J. van Benthem, and F. Wolter, editors. *Handbook of Modal Logic*, volume 3 of *Studies in Logic and Practical Reasoning*. Elsevier, 2007.
- [Doš84] K. Došen. Intuitionistic double negation as a necessity operator. *Publications de l'Institut Mathématique (Beograd)*, 35(49), 1984.

- [dPR11] V. de Paiva and E. Ritter. *Logic without Frontiers: Festschrift for Walter Alexandre Carnielli on the occasion of his 60th birthday*, volume 17 of *Tributes*, chapter Basic Constructive Modality. College Publications, 2011.
- [Fef89] S. Feferman. *The Number Systems: Foundations of Algebra and Analysis*. AMS Chelsea Publishing, second edition, 1964 (1989). Reprinted by the American Mathematical Society, 2003.
- [FHMV95] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.
- [Fis84] G. Fischer Servi. Axiomatisations for some intuitionistic modal logics. *Rendiconti del seminario matematico del Politecnico di Torino*, 42(3), 1984.
- [Fit07] M. Fitting. *Handbook of Modal Logic*, chapter Modal Proof Theory. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [FSK10] N. Ferguson, B. Schneier, and T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 2010.
- [Gab95] D.M. Gabbay, editor. *What Is a Logical System?* Number 4 in *Studies in Logic and Computation*. Oxford University Press, 1995.
- [GO07] V. Goranko and M. Otto. *Handbook of Modal Logic*, chapter Model Theory of Modal Logic. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [Gol11] D. Gollmann. *Computer Security*. Wiley, third edition, 2011.
- [HR10] V.F. Hendricks and O. Roy, editors. *Epistemic Logic: 5 Questions*. Automatic Press, 2010.
- [Hru07] P. Hrubeš. A lower bound for intuitionistic logic. *Annals of Pure and Applied Logic*, 146, 2007.
- [Jeř08] E. Jeřábek. Independent bases of admissible rules. *Logic Journal of the Interest Group in Pure and Applied Logic*, 16(3), 2008.
- [Kra12a] S. Kramer. A logic of interactive proofs (formal theory of knowledge transfer). Technical Report 1201.3667, arXiv, 2012. <http://arxiv.org/abs/1201.3667>.
- [Kra12b] S. Kramer. Logic of negation-complete interactive proofs (formal theory of epistemic deciders). Technical Report 1208.5913, arXiv, 2012. <http://arxiv.org/abs/1208.5913>.
- [Kra12c] S. Kramer. Logic of non-monotonic interactive proofs (formal theory of temporary knowledge transfer). Technical Report 1208.1842, arXiv, 2012. <http://arxiv.org/abs/1208.1842>.

- [Kra13a] S. Kramer. Logic of intuitionistic interactive proofs (formal theory of disjunctive knowledge transfer). Short paper presented at the Congress on Logic and Philosophy of Science, Ghent, 2013.
- [Kra13b] S. Kramer. Logic of negation-complete interactive proofs (formal theory of epistemic deciders). In *Proceedings of IMLA*, volume 300 of *ENTCS*. Elsevier, 2013.
- [Kra13c] S. Kramer. Logic of non-monotonic interactive proofs. In *Proceedings of ICLA*, volume 7750 of *LNCS*. Springer, 2013.
- [Kri65] S.A. Kripke. *Formal Systems and Recursive Functions*, volume 40 of *Studies in Logic and the Foundations of Mathematics*, chapter Semantical Analysis of Intuitionistic Logic I. Elsevier, 1965.
- [Mos06] Y. Moschovakis. *Notes on Set Theory*. Springer, 2nd edition, 2006.
- [Mos10] J. Moschovakis. Intuitionistic logic. In *The Stanford Encyclopedia of Philosophy*. Summer 2010 edition, 2010.
- [MV07] J.-J. Meyer and F. Veltman. *Handbook of Modal Logic*, chapter Intelligent Agents and Common Sense Reasoning. Volume 3 of Blackburn et al. [BvBW07], 2007.
- [PP13] K. Pouliasis and G. Primiero. J-Calc: A typed lambda calculus for Intuitionistic Justification Logic. In *Proceedings of IMLA*, volume 300 of *ENTCS*. Elsevier, 2013.
- [PS86] G. Plotkin and C. Stirling. A framework for intuitionistic modal logics. In *Proceedings of the Conference on Theoretical Aspects of Rationality and Knowledge*. Morgan Kaufmann Publishers Inc., 1986.
- [Ran10] K. Ranalter. Embedding constructive K into intuitionistic K. *Electronic Notes in Theoretical Computer Science*, 262, 2010.
- [SB13] G. Steren and E. Bonelli. Intuitionistic Hypothetical Logic of Proofs. In *Proceedings of IMLA*, volume 300 of *ENTCS*. Elsevier, 2013.
- [Sim94] A.K. Simpson. *The Proof-Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, University of Edinburgh, 1994.
- [Sta79] R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9, 1979.
- [Tay99] P. Taylor. *Practical Foundations of Mathematics*. Cambridge University Press, 1999.
- [TGD10] A. Tiu, R. Goré, and J. Dawson. A proof theoretic analysis of intruder theories. *Logical Methods in Computer Science*, 6(3), 2010.

- [vB97] J. van Benthem. *Logic and Reality: Essays on the Legacy of Arthur Prior*, chapter Modal Logic as a Theory of Information. Clarendon Press, Oxford, 1997.
- [vB09] J. van Benthem. The information in intuitionistic logic. *Synthese*, 167, 2009.
- [Wij90] D. Wijesekera. Constructive modal logic I. *Annals of Pure and Applied Logic*, 50, 1990.

## A Remaining proofs

### A.1 Proof of Theorem 2

For 0, combine MM and MP. For 1–6, 8–9, and 32–35, consult their analogs and their proofs in LiP [Kra12a]; they require no non-intuitionistic machinery. For 7, apply ID to 6. For 10, combine ET and MM. For 11, consider that:

1.  $\vdash_{\text{LiP}} M \pm_{\text{CM}} \text{CM k } M$  self-knowledge
2.  $\vdash_{\text{LiP}} (M \pm_{\text{CM}} \text{CM k } M) \rightarrow M \mp_{\text{CM}} \text{CM k } M$  ID
3.  $\vdash_{\text{LiP}} (M \mp_{\text{CM}} \text{CM k } M) \leftrightarrow \neg\neg(\text{CM k } M \wedge \text{CM k } M)$  definition
4.  $\vdash_{\text{LiP}} \neg\neg(\text{CM k } M \wedge \text{CM k } M) \leftrightarrow \neg\neg(\text{CM k } M)$  IL
5.  $\vdash_{\text{LiP}} \neg\neg(\text{CM k } M)$  1–4, IL.

For 12, consider that:

1.  $\vdash_{\text{LiP}} \text{CM k } M \rightarrow ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  ET *bis*
2.  $\vdash_{\text{LiP}} \neg\neg(\text{CM k } M)$  CMMC
3.  $\vdash_{\text{LiP}} \neg\neg((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  1, 2, IL.

For 13, consider that:

1.  $\vdash_{\text{LiP}} \neg\phi \rightarrow \neg(\text{CM k } M \wedge \phi)$  IL
2.  $\vdash_{\text{LiP}} \neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg\neg\neg(\text{CM k } M \wedge \phi)$  IL (triple-negation law)
3.  $\vdash_{\text{LiP}} \neg\neg\neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg(M \mp_{\text{CM}} \phi)$  definition
4.  $\vdash_{\text{LiP}} \neg\phi \rightarrow \neg(M \mp_{\text{CM}} \phi)$  1–3, IL.

For 14, consider that:

1.  $\vdash_{\text{LiP}} \neg(M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg\neg(\text{CM k } M \wedge \phi)$  definition
2.  $\vdash_{\text{LiP}} \neg\neg\neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg(\text{CM k } M \wedge \phi)$  IL (triple-negation law)
3.  $\vdash_{\text{LiP}} \neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg(\text{CM k } M \wedge M \pm_{\text{CM}} \phi)$  2, ET *bis*, IL



4.  $\vdash_{\text{LHP}} \neg(\text{CM k } M \wedge M \pm_{\text{CM}} \phi) \leftrightarrow ((M \pm_{\text{CM}} \phi) \rightarrow \neg(\text{CM k } M))$  IL
5.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \rightarrow \neg(\text{CM k } M)) \leftrightarrow ((M \pm_{\text{CM}} \phi) \rightarrow \perp)$  4, CMMC, IL
6.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \rightarrow \perp) \leftrightarrow \neg(M \pm_{\text{CM}} \phi)$  IL
7.  $\vdash_{\text{LHP}} \neg(M \mp_{\text{CM}} \phi) \leftrightarrow \neg(M \pm_{\text{CM}} \phi)$  1–6, IL.

For 15, inspect 13 and 14. And 16, 17, and 18, are instances of 13, 14, and 15.

For 19, consider ID as well as 16 and 18, and that:

1.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg(\text{CM k } M \wedge \phi)$  definition
2.  $\vdash_{\text{LHP}} \neg\neg(\text{CM k } M \wedge \phi) \rightarrow (\neg\neg(\text{CM k } M) \wedge \neg\neg\phi)$  IL
3.  $\vdash_{\text{LHP}} (\neg\neg(\text{CM k } M) \wedge \neg\neg\phi) \rightarrow \neg\neg\phi$  IL
4.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow \neg\neg\phi$  1–3, IL.

For 20, consider that:

1.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow \neg\neg\phi$  EWDN
2.  $\vdash_{\text{LHP}} \phi' \rightarrow M \pm_{\text{CM}} \phi'$  MM
3.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi') \rightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi')$  1, 2, IL.

For 21, consider that:

1.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi) \rightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi)$  CF
2.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi$  ID
3.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi) \rightarrow ((M \mp_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} \phi)$  1, 2, IL.

For 22, inspect ET *bis*; for 23, 22 and 21; for 24 and 25,  $\vdash_{\text{LHP}} \neg\perp$  and 15 and 13, respectively; for 26, MM and ID. For 27, suppose that  $\vdash_{\text{LHP}} \text{CM k } M \rightarrow \phi$ . Hence,  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \text{CM k } M) \rightarrow M \pm_{\text{CM}} \phi$  by R, and  $\vdash_{\text{LHP}} M \pm_{\text{CM}} \phi$  by self-knowledge. Conversely suppose that  $\vdash_{\text{LHP}} M \pm_{\text{CM}} \phi$ . Hence  $\vdash_{\text{LHP}} \text{CM k } M \rightarrow \phi$  by ET. For 28, instantiate  $\phi$  in 27 with  $\text{CM k } M'$ . For 29, inspect 10 and 27, and for 30 and 31, MM. For 36, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)$  (4)
2.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  ET *bis* self-proof
3.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} (((M \pm_{\text{CM}} \phi) \rightarrow \phi) \wedge (\phi \rightarrow M \pm_{\text{CM}} \phi))$  2, definition
4.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} ((M \pm_{\text{CM}} \phi) \rightarrow \phi)$  3, proof conjunctions *bis*
5.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} ((M \pm_{\text{CM}} \phi) \rightarrow \phi)) \rightarrow ((M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \rightarrow M \pm_{\text{CM}} \phi)$  K
6.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \rightarrow M \pm_{\text{CM}} \phi$  4, 5, IL

$$7. \vdash_{\text{LIIP}} (M \pm_{\text{CM}} (M \pm_{\text{CM}} \phi)) \leftrightarrow M \pm_{\text{CM}} \phi \quad 1, 6, \text{IL.}$$

For 37, consider that:

$$\begin{aligned} 1. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow \neg\neg(\text{CM } k M \wedge \neg\neg(\text{CM } k M \wedge \phi)) && \text{definition} \\ 2. & \vdash_{\text{LIIP}} \neg\neg(\text{CM } k M \wedge \neg\neg(\text{CM } k M \wedge \phi)) \rightarrow && \text{IL} \\ & (\neg\neg(\text{CM } k M) \wedge \neg\neg\neg\neg(\text{CM } k M \wedge \phi)) \\ 3. & \vdash_{\text{LIIP}} (\neg\neg(\text{CM } k M) \wedge \neg\neg\neg\neg(\text{CM } k M \wedge \phi)) \rightarrow \neg\neg\neg\neg(\text{CM } k M \wedge \phi) && \text{IL} \\ 4. & \vdash_{\text{LIIP}} \neg\neg\neg\neg(\neg(\text{CM } k M \wedge \phi)) \leftrightarrow \neg(\neg(\text{CM } k M \wedge \phi)) && \text{IL (triple-negation law)} \\ 5. & \vdash_{\text{LIIP}} \neg\neg(\text{CM } k M \wedge \phi) \leftrightarrow M \mp_{\text{CM}} \phi && \text{definition} \\ 6. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} \phi && 1-5, \text{IL} \\ 7. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi) && \text{WMM} \\ 8. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow M \mp_{\text{CM}} \phi && 6, 7, \text{IL.} \end{aligned}$$

For 38, consider MM, ID, and that:

$$\begin{aligned} 1. & \vdash_{\text{LIIP}} \phi \rightarrow M \pm_{\text{CM}} \phi && \text{MM} \\ 2. & \vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && \text{WMM} \\ 3. & \vdash_{\text{LIIP}} \phi \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && 1, 2, \text{IL.} \end{aligned}$$

and also that:

$$\begin{aligned} 1. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg(\text{CM } k M \wedge \phi) && \text{definition} \\ 2. & \vdash_{\text{LIIP}} \text{CM } k M \rightarrow ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi) && \text{ET } bis \\ 3. & \vdash_{\text{LIIP}} \neg\neg(\text{CM } k M \wedge \phi) \leftrightarrow \neg\neg(\text{CM } k M \wedge M \pm_{\text{CM}} \phi) && 2, \text{IL} \\ 4. & \vdash_{\text{LIIP}} \neg\neg(\text{CM } k M \wedge M \pm_{\text{CM}} \phi) \leftrightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && \text{definition} \\ 5. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} \phi) \leftrightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && 1, 3, 4, \text{IL.} \end{aligned}$$

For 39, consider that:

$$\begin{aligned} 1. & \vdash_{\text{LIIP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi) && \text{ID} \\ 2. & \vdash_{\text{LIIP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} \phi && \text{MI } bis \\ 3. & \vdash_{\text{LIIP}} M \mp_{\text{CM}} \phi \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && \text{NMM} \\ 4. & \vdash_{\text{LIIP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi) && 1-3, \text{IL.} \end{aligned}$$

For 40, consider the instance  $\vdash_{\text{LIIP}} \text{CM } k M \rightarrow ((M \pm_{\text{CM}} (\phi \vee \phi')) \rightarrow (\phi \vee \phi'))$  of ET *bis*, and that  $\vdash_{\text{LIIP}} (\phi \vee \phi') \rightarrow ((M \pm_{\text{CM}} \phi) \vee M \pm_{\text{CM}} \phi')$  by MM. Hence  $\vdash_{\text{LIIP}} \text{CM } k M \rightarrow ((M \pm_{\text{CM}} (\phi \vee \phi')) \rightarrow ((M \pm_{\text{CM}} \phi) \vee M \pm_{\text{CM}} \phi'))$ . For 41, consider 27 and 40. For 42, consider that:

1.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)) \rightarrow ((M \pm_{\text{CM}} \text{CM k } M) \wedge M \pm_{\text{CM}} \phi)$  pr. conj. *bis*
2.  $\vdash_{\text{LIIP}} ((M \pm_{\text{CM}} \text{CM k } M) \wedge M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi$  IL
3.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)) \rightarrow M \pm_{\text{CM}} \phi$  1, 2, IL
4.  $\vdash_{\text{LIIP}} M \pm_{\text{CM}} \text{CM k } M$  self-knowledge
5.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi$  IL
6.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \rightarrow ((M \pm_{\text{CM}} \text{CM k } M) \wedge M \pm_{\text{CM}} \phi)$  4, 5, IL
7.  $\vdash_{\text{LIIP}} ((M \pm_{\text{CM}} \text{CM k } M) \wedge M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)$  pr. conj. *bis*
8.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)$  6, 7, IL
9.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)$  3, 8, IL.

For 43, consider that :

1.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge \phi)$  EI
2.  $\vdash_{\text{LIIP}} \text{CM k } M \rightarrow ((M \pm_{\text{CM}} \phi) \leftrightarrow \phi)$  ET *bis*
3.  $\vdash_{\text{LIIP}} (\text{CM k } M \wedge \phi) \leftrightarrow (\text{CM k } M \wedge M \pm_{\text{CM}} \phi)$  2, IL
4.  $\vdash_{\text{LIIP}} M \pm_{\text{CM}} (\text{CM k } M \wedge \phi) \leftrightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge M \pm_{\text{CM}} \phi)$  3, R *bis*
5.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} \phi) \leftrightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge M \pm_{\text{CM}} \phi)$  1, 4, IL.

For 44, consider that:

1.  $\vdash_{\text{LIIP}} (M \mp_{\text{CM}} (\phi \vee \phi')) \leftrightarrow \neg\neg(\text{CM k } M \wedge (\phi \vee \phi'))$  definition
2.  $\vdash_{\text{LIIP}} \neg\neg(\text{CM k } M \wedge (\phi \vee \phi')) \leftrightarrow \neg\neg((\text{CM k } M \wedge \phi) \vee (\text{CM k } M \wedge \phi'))$  IL
3.  $\vdash_{\text{LIIP}} \neg\neg((\text{CM k } M \wedge \phi) \vee (\text{CM k } M \wedge \phi')) \leftrightarrow \neg\neg(\neg\neg(\text{CM k } M \wedge \phi) \vee \neg\neg(\text{CM k } M \wedge \phi'))$  IL
4.  $\vdash_{\text{LIIP}} (M \mp_{\text{CM}} (\phi \vee \phi')) \leftrightarrow (\neg\neg(\text{CM k } M \wedge \phi) \vee \neg\neg(\text{CM k } M \wedge \phi'))$  1–3, IL
5.  $\vdash_{\text{LIIP}} (M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg(\text{CM k } M \wedge \phi)$  definition
6.  $\vdash_{\text{LIIP}} (M \mp_{\text{CM}} \phi') \leftrightarrow \neg\neg(\text{CM k } M \wedge \phi')$  definition
7.  $\vdash_{\text{LIIP}} (M \mp_{\text{CM}} (\phi \vee \phi')) \leftrightarrow ((M \mp_{\text{CM}} \phi) \vee M \mp_{\text{CM}} \phi')$  4, 5, 6, IL.

For 45, consider that:

1.  $\vdash_{\text{LIIP}} (M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow (\text{CM k } M \rightarrow (\phi \rightarrow \phi'))$  ET
2.  $\vdash_{\text{LIIP}} (\text{CM k } M \rightarrow (\phi \rightarrow \phi')) \leftrightarrow ((\text{CM k } M \rightarrow \phi) \rightarrow (\text{CM k } M \rightarrow \phi'))$  IL
3.  $\vdash_{\text{LIIP}} ((\text{CM k } M \rightarrow \phi) \rightarrow (\text{CM k } M \rightarrow \phi')) \rightarrow ((\text{CM k } M \wedge (\text{CM k } M \rightarrow \phi)) \rightarrow (\text{CM k } M \wedge (\text{CM k } M \rightarrow \phi')))$  IL

4.  $\vdash_{\text{LHP}} ((\text{CM k } M \wedge (\text{CM k } M \rightarrow \phi)) \rightarrow (\text{CM k } M \wedge (\text{CM k } M \rightarrow \phi'))) \leftrightarrow ((\text{CM k } M \wedge \phi) \rightarrow (\text{CM k } M \wedge \phi'))$  IL
5.  $\vdash_{\text{LHP}} ((\text{CM k } M \wedge \phi) \rightarrow (\text{CM k } M \wedge \phi')) \rightarrow (\neg\neg(\text{CM k } M \wedge \phi) \rightarrow \neg\neg(\text{CM k } M \wedge \phi'))$  IL
6.  $\vdash_{\text{LHP}} (\neg\neg(\text{CM k } M \wedge \phi) \rightarrow \neg\neg(\text{CM k } M \wedge \phi')) \leftrightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi')$  definition
7.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi')$  1–6, IL.

For 46, consider that:

1.  $\vdash_{\text{LHP}} \phi \rightarrow M \mp_{\text{CM}} \phi$  WMM
2.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi') \rightarrow (\text{CM k } M \rightarrow \phi')$  ET
3.  $\vdash_{\text{LHP}} ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi') \rightarrow (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))$  1, 2, IL
4.  $\vdash_{\text{LHP}} (\phi \rightarrow (\text{CM k } M \rightarrow \phi')) \rightarrow M \pm_{\text{CM}} (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))$  MM
5.  $\vdash_{\text{LHP}} ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi') \rightarrow M \pm_{\text{CM}} (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))$  3, 4, IL
6.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))) \leftrightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge (\phi \rightarrow (\text{CM k } M \rightarrow \phi')))$  EI
7.  $\vdash_{\text{LHP}} ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi') \rightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge (\phi \rightarrow (\text{CM k } M \rightarrow \phi')))$  5, 6, IL
8.  $\vdash_{\text{LHP}} (\text{CM k } M \wedge (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))) \rightarrow (\phi \rightarrow \phi')$  IL
9.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} (\text{CM k } M \wedge (\phi \rightarrow (\text{CM k } M \rightarrow \phi'))) \rightarrow M \pm_{\text{CM}} (\phi \rightarrow \phi')$  8, R
10.  $\vdash_{\text{LHP}} ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi') \rightarrow M \pm_{\text{CM}} (\phi \rightarrow \phi')$  7, 9, IL.

For 47, inspect CF and PS5. For 48, consider that:

1.  $\vdash_{\text{LHP}} (\neg\neg\phi \rightarrow \phi') \rightarrow ((M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi')$  CF
2.  $\vdash_{\text{LHP}} (\neg\neg\phi' \rightarrow \phi) \rightarrow ((M \mp_{\text{CM}} \phi') \rightarrow M \pm_{\text{CM}} \phi)$  CF
3.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (\phi \vee \phi')) \leftrightarrow ((M \mp_{\text{CM}} \phi) \vee M \mp_{\text{CM}} \phi')$  PS4
4.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\phi \vee \phi')) \rightarrow M \mp_{\text{CM}} (\phi \vee \phi')$  ID
5.  $\vdash_{\text{LHP}} ((\neg\neg\phi \rightarrow \phi') \wedge (\neg\neg\phi' \rightarrow \phi)) \rightarrow ((M \pm_{\text{CM}} (\phi \vee \phi')) \rightarrow ((M \pm_{\text{CM}} \phi) \vee M \pm_{\text{CM}} \phi'))$  1–4, IL.

For 49, consider that  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  by MM; thus  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  by ID; and thus  $\vdash_{\text{LHP}} \phi \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  by MM. For 50, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi$  ID

2.  $\vdash_{\text{LHP}} M \pm_{\text{CM}} ((M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi)$  1, N
3.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)$  2, PS2
4.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} \phi$  MI *bis*
5.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  MM
6.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (M \pm_{\text{CM}} \phi)) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  3–5, IL.

For 51, combine MS and MS *bis*. For 52, consider the in fact stronger-than-necessary proof of 38. For 53, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)$  ID
2.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow M \mp_{\text{CM}} \phi$  MI *bis*
3.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \rightarrow M \mp_{\text{CM}} \phi$  1, 2, IL
4.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  MM
5.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow M \mp_{\text{CM}} \phi$  3, 4 IL.

For 54, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow M \pm_{\text{CM}} (\text{CM k } M \wedge \neg\neg\phi)$  EI
2.  $\vdash_{\text{LHP}} (\text{CM k } M \wedge \neg\neg\phi) \rightarrow \neg\neg(\text{CM k } M \wedge \phi)$  IL
3.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\text{CM k } M \wedge \neg\neg\phi)) \rightarrow M \pm_{\text{CM}} \neg\neg(\text{CM k } M \wedge \phi)$  2, R
4.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow M \pm_{\text{CM}} \neg\neg(\text{CM k } M \wedge \phi)$  1, 3, IL
5.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg(\text{CM k } M \wedge \phi)) \leftrightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  definition
6.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)$  4, 5, IL
7.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (M \mp_{\text{CM}} \phi)) \leftrightarrow M \mp_{\text{CM}} \phi$  MMI *bis*
8.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow M \mp_{\text{CM}} \phi$  6, 7, IL.

For 55, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow M \mp_{\text{CM}} \phi$  DNA
2.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow \neg\neg\phi$  EWDN
3.  $\vdash_{\text{LHP}} \phi \rightarrow M \pm_{\text{CM}} \phi$  MM
4.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow (\neg\neg\phi \wedge (\phi \rightarrow M \pm_{\text{CM}} \phi))$  2, 3, IL
5.  $\vdash_{\text{LHP}} (\neg\neg\phi \wedge (\phi \rightarrow M \pm_{\text{CM}} \phi)) \rightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  IL
6.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \neg\neg\phi) \rightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  1, 4, 5, IL.

For 56, consider that:

1.  $\vdash_{\text{LHP}} \neg(M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg\neg(\text{CM k } M \wedge \phi)$  definition
2.  $\vdash_{\text{LHP}} \neg\neg\neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg(\text{CM k } M \wedge \phi)$  IL (triple-negation law)
3.  $\vdash_{\text{LHP}} \neg(\text{CM k } M \wedge \phi) \leftrightarrow (\text{CM k } M \rightarrow \neg\phi)$  IL
4.  $\vdash_{\text{LHP}} \neg\neg(\text{CM k } M)$  CMMC
5.  $\vdash_{\text{LHP}} (\text{CM k } M \rightarrow \neg\phi) \leftrightarrow (\neg\neg(\text{CM k } M) \wedge (\text{CM k } M \rightarrow \neg\phi))$  4, IL
6.  $\vdash_{\text{LHP}} (\neg\neg(\text{CM k } M) \wedge (\text{CM k } M \rightarrow \neg\phi)) \rightarrow \neg\neg(\text{CM k } M \wedge \neg\phi)$  IL
7.  $\vdash_{\text{LHP}} \neg\neg(\text{CM k } M \wedge \neg\phi) \leftrightarrow M \mp_{\text{CM}} \neg\phi$  definition
8.  $\vdash_{\text{LHP}} \neg(M \mp_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \neg\phi$  1–7, IL.

For 57, combine FNDETU and WNC. For 58, consider that:

1.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow \neg\neg\phi$  EWDN
2.  $\vdash_{\text{LHP}} \phi \rightarrow M \pm_{\text{CM}} \phi$  MM
3.  $\vdash_{\text{LHP}} (\neg\neg\phi \wedge (\phi \rightarrow M \pm_{\text{CM}} \phi)) \rightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  IL
4.  $\vdash_{\text{LHP}} \neg\neg\phi \rightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  2, 3, IL
5.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \rightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  1, 4, IL
6.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi$  ID
7.  $\vdash_{\text{LHP}} (\neg\neg(M \pm_{\text{CM}} \phi) \wedge ((M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi)) \rightarrow \neg\neg(M \mp_{\text{CM}} \phi)$  IL
8.  $\vdash_{\text{LHP}} \neg\neg(M \pm_{\text{CM}} \phi) \rightarrow \neg\neg(M \mp_{\text{CM}} \phi)$  6, 7, IL
9.  $\vdash_{\text{LHP}} \neg\neg(M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg\neg\neg(\text{CM k } M \wedge \phi)$  definition
10.  $\vdash_{\text{LHP}} \neg\neg\neg\neg(\text{CM k } M \wedge \phi) \leftrightarrow \neg\neg(\text{CM k } M \wedge \phi)$  triple-negation law
11.  $\vdash_{\text{LHP}} \neg\neg(\text{CM k } M \wedge \phi) \leftrightarrow M \mp_{\text{CM}} \phi$  definition
12.  $\vdash_{\text{LHP}} \neg\neg(M \pm_{\text{CM}} \phi) \rightarrow M \mp_{\text{CM}} \phi$  8–11, IL
13.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} \phi) \leftrightarrow \neg\neg(M \pm_{\text{CM}} \phi)$  5, 12, IL.

For 59, consider that:

1.  $\vdash_{\text{LHP}} (M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \pm_{\text{CM}} \phi) \rightarrow M \pm_{\text{CM}} \phi')$  K
2.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \wedge M \mp_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow ((M \pm_{\text{CM}} (\phi \rightarrow \phi')) \rightarrow M \pm_{\text{CM}} \phi') \wedge M \mp_{\text{CM}} (\phi \rightarrow \phi')$  1, IL
3.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}} (\phi \rightarrow \phi')) \leftrightarrow \neg\neg(M \pm_{\text{CM}} (\phi \rightarrow \phi'))$  MDN

4.  $\vdash_{\text{LHP}} (((M \pm_{\text{CM}}(\phi \rightarrow \phi')) \rightarrow M \pm_{\text{CM}} \phi') \wedge M \mp_{\text{CM}}(\phi \rightarrow \phi')) \leftrightarrow$   
 $((M \pm_{\text{CM}}(\phi \rightarrow \phi')) \rightarrow M \pm_{\text{CM}} \phi') \wedge \neg\neg(M \pm_{\text{CM}}(\phi \rightarrow \phi')))$  3, IL
5.  $\vdash_{\text{LHP}} (((M \pm_{\text{CM}}(\phi \rightarrow \phi')) \rightarrow M \pm_{\text{CM}} \phi') \wedge \neg\neg(M \pm_{\text{CM}}(\phi \rightarrow \phi')) \rightarrow$   
 $\neg\neg(M \pm_{\text{CM}} \phi'))$  IL
6.  $\vdash_{\text{LHP}} \neg\neg(M \pm_{\text{CM}} \phi') \leftrightarrow M \mp_{\text{CM}} \phi'$  MDN
7.  $\vdash_{\text{LHP}} ((M \pm_{\text{CM}} \phi) \wedge M \mp_{\text{CM}}(\phi \rightarrow \phi')) \rightarrow M \mp_{\text{CM}} \phi'$  2, 4, 5, 6, IL.

For 60, consider that:

1.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}}(\phi \wedge \neg\phi)) \rightarrow \neg\neg(\phi \wedge \neg\phi)$  EWDN
2.  $\vdash_{\text{LHP}} \neg\neg(\phi \wedge \neg\phi) \rightarrow (\neg(\phi \wedge \neg\phi) \rightarrow (\phi \wedge \neg\phi))$  IL (*reductio ad absurdum*)
3.  $\vdash_{\text{LHP}} \perp \rightarrow \perp$  IL
4.  $\vdash_{\text{LHP}} (\perp \rightarrow \perp) \leftrightarrow \neg\perp$  IL
5.  $\vdash_{\text{LHP}} \neg\perp \leftrightarrow \neg(\phi \wedge \neg\phi)$  IL
6.  $\vdash_{\text{LHP}} \neg(\phi \wedge \neg\phi)$  3, 4, 5, IL
7.  $\vdash_{\text{LHP}} \neg\neg(\phi \wedge \neg\phi) \rightarrow (\phi \wedge \neg\phi)$  2, 6, IL
8.  $\vdash_{\text{LHP}} (M \mp_{\text{CM}}(\phi \wedge \neg\phi)) \rightarrow (\phi \wedge \neg\phi)$  1, 7, IL.

## A.2 Finite-model property

- $\sqsubseteq^{\text{min}, \Gamma}$  inherits the reflexivity, transitivity, and anti-symmetry from  $\sqsubseteq$  as can be seen by inspecting the definition of  $\sqsubseteq^{\text{min}, \Gamma}$ ;
- $M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma}$  inherits seriality from  $M\mathcal{R}_{\text{CM}}$ , as can be seen by inspecting the definition of  $M\mathcal{R}_a^{\text{min}, \Gamma}$ ;
- for conditional reflexivity of  $M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma}$ , suppose that  $M \in \text{cl}_{\text{CM}}^{[s] \sim_{\Gamma}}(\emptyset)$ . Thus consecutively:  $[s] \sim_{\Gamma} \in \mathcal{V}_{\Gamma}(\text{CMk} M)$  by definition,  $s \in \mathcal{V}(\text{CMk} M)$  by definition,  $M \in \text{cl}_{\text{CM}}^s(\emptyset)$  by definition,  $s M\mathcal{R}_{\text{CM}} s$  by the conditional reflexivity of  $M\mathcal{R}_{\text{CM}}$ , and finally  $[s] \sim_{\Gamma} M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma} [s] \sim_{\Gamma}$  by definition;
- for the epistemic-image property of  $M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma}$ , suppose that  $[s] \sim_{\Gamma} M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma} [s'] \sim_{\Gamma}$ . Thus consecutively:  $s M\mathcal{R}_{\text{CM}} s'$  by definition,  $M \in \text{cl}_{\text{CM}}^{s'}(\emptyset)$  by the epistemic-image property of  $M\mathcal{R}_{\text{CM}}$ ,  $s' \in \mathcal{V}(\text{CMk} M)$  by definition,  $[s'] \sim_{\Gamma} \in \mathcal{V}_{\Gamma}(\text{CMk} M)$  by definition, and finally  $M \in \text{cl}_{\text{CM}}^{[s'] \sim_{\Gamma}}(\emptyset)$  by definition.
- For the MIAR-inclusion property of  $M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma}$ , suppose that:
  - $[s] \sim_{\Gamma} M\mathcal{R}_{\text{CM}}^{\text{min}, \Gamma} [s'] \sim_{\Gamma}$ . Thus consecutively:  $s M\mathcal{R}_{\text{CM}} s'$  by definition,  $s \sqsubseteq s'$  by MIAR-inclusion, and  $[s] \sim_{\Gamma} \sqsubseteq^{\text{min}, \Gamma} [s'] \sim_{\Gamma}$  by definition. Proceed similarly for the converse.

- $[s]_{\sim_{\Gamma}} M\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$ . Thus consecutively:  $s M\mathcal{R}_{\text{CM}} s'$  by definition,  $s {}_{\text{CM}}\mathcal{R}_{\text{CM}} s'$  by MIAR-inclusion, and  $[s]_{\sim_{\Gamma}} {}_{\text{CM}}\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$  by definition.

- For the special transitivity of  $M\mathcal{R}_{\text{CM}}^{\min, \Gamma}$ , suppose that

$$[s]_{\sim_{\Gamma}} ({}_{\text{CM}}\mathcal{R}_{\text{CM}}^{\min, \Gamma} \circ M\mathcal{R}_{\text{CM}}^{\min, \Gamma}) [s']_{\sim_{\Gamma}}.$$

That is, there is  $[s''] \in \mathcal{S}/_{\sim_{\Gamma}}$  such that

- $[s]_{\sim_{\Gamma}} {}_{\text{CM}}\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s'']_{\sim_{\Gamma}}$  and
- $[s'']_{\sim_{\Gamma}} M\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$ .

Thus consecutively:  $s {}_{\text{CM}}\mathcal{R}_{\text{CM}} s''$  and  $s'' M\mathcal{R}_{\text{CM}} s'$  by definition,  $s M\mathcal{R}_{\text{CM}} s''$  by MIAR-inclusion, and  $[s]_{\sim_{\Gamma}} M\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$  by definition.

- For the proof monotonicity of  $M\mathcal{R}_{\text{CM}}^{\min, \Gamma}$ , suppose that  $M \sqsubseteq_{\text{CM}} M'$ . Further suppose that  $[s]_{\sim_{\Gamma}} M\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$ . Thus consecutively:  $s M\mathcal{R}_{\text{CM}} s'$  by definition,  $s M'\mathcal{R}_{\text{CM}} s'$  by proof monotonicity, and  $[s]_{\sim_{\Gamma}} M'\mathcal{R}_{\text{CM}}^{\min, \Gamma} [s']_{\sim_{\Gamma}}$  by definition.